OBSERVATORIO DE LA
CIBERSEGURIDAD
EN AMÉRICA LATINA Y EL CARIBE

Ciberseguridad

¿Estamos preparados en América Latina y el Caribe?

Informe Ciberseguridad 2016

www.observatoriociberseguridad.com

Organization of American States
More rights for more people

BID
Mejorando vidas

Organization of
American States
More rights for more people

Banco Interamericano de Desarrollo

Luis Alberto Moreno
Presidente

Coordinación del Proyecto

Miguel Porrúa
Especialista Líder de Gobierno Electrónico

BID-OEA Equipo Técnico

Kerry-Ann Barrett
Robert Fain
Catalina García
Gonzalo García-Belenguer
Catalina Lillo
Bárbara Marchiori
Emmanuelle Pelletier
Diego Subero

Organización de los Estados Americanos

Luis Almagro
Secretario General

Coordinación del Proyecto

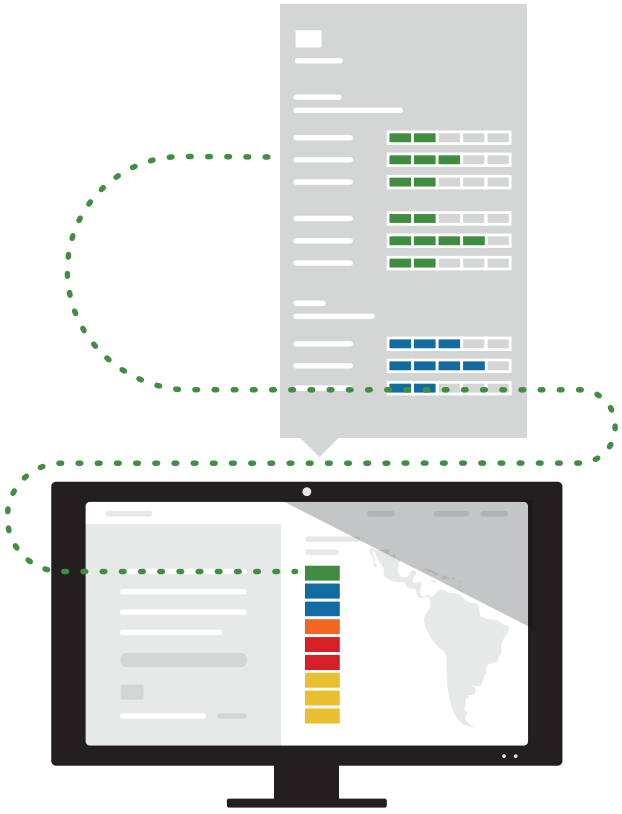
Belisario Contreras
Gerente del Programa de Seguridad Cibernética

Centro Global de Capacitación de Seguridad Cibernética - Universidad de Oxford

Prof. Sadie Creese
Prof. Michael Goldsmith
Dr. María Bada
Taylor Roberts
Lara Pace

Tabla de contenidos

Mensajes institucionales



Contribuciones de expertos

Marco metodológico

Perfiles de países

Apéndice: marco metodológico detallado

www.observatoriociberseguridad.com

El set de datos también puede ser descargado en formato abierto en: https://mydata.iadb.org/idb/dataset/cd6z-sjjc

Lista de acrónimos

ADSIB
Agencia para el Desarrollo de la Sociedad de la Información en Bolivia

APWG
Grupo de Trabajo Anti-Phishing

ALC
América Latina y el Caribe

AusCERT
Equipo de Respuesta de Emergencia Informática de Australia

BID
Banco Interamericano de Desarrollo

CARICOM
Comunidad del Caribe

CGi.br
Comité Gestor de Internet en Brasil

CMM
Modelo de Madurez de Capacidad de Ciberseguridad

CoE
Consejo de Europa

CONATEL
Consejo Nacional de Telecomunicaciones de Haití

CONICYT
Consejo Nicaragüense de Ciencia y Tecnología

CSIRT
Equipo de respuesta ante incidentes de seguridad cibernética

CSIS
Centro de Estudios Estratégicos e Internacionales

CTU
Unión de Telecomunicaciones del Caribe

DDoS
Ataques de denegación de servicio distribuidos

DoS
Denegación de servicio

DUDH
Declaración Universal de Derechos Humanos

FGV
Fundación Getúlio Vargas

FIRST
Foro de Equipos de Respuesta ante Incidentes y de Seguridad

GCCS
Conferencia Mundial sobre el Espacio Cibernético

GCSCC
Centro Global de Capacidad sobre Seguridad Cibernética (Oxford)

GGE
Grupo de Expertos Gubernamentales de las Naciones Unidas

ICANN
Corporación de Internet para Nombres y Números Asignados

ICIC
Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad

ICN
Infraestructuras críticas nacionales

IFD
Departamento de Instituciones para el Desarrollo del BID

IGF
Foro de Gobernanza de Internet

IITCUP
División Informática Forense del Instituto de Investigaciones Técnico Científicas de la Universidad Policial (Bolivia)

IXP
Punto de intercambio de Internet

LACNIC
Centro de Información de la Red de América Latina y el Caribe

Metas SMART
Metas específicas, evaluables, realistas y con un tiempo definido

MFC
Medidas de fomento de la confianza

MICITT
Ministerio de Ciencia, Tecnología y Telecomunicaciones de Costa Rica

MMWG
Grupo de Trabajo de Modelado Plurirregional

NCI
Instituto Nacional de Ciberseguridad

NIC.br
Centro de Información de la Red Brasileña

OEA
Organización de los Estados Americanos

ONGEI
Oficina Nacional de Gobierno Electrónico e Informática (Perú)

OSCE
Organización de Seguridad y Cooperación en Europa

PIB
Producto interno bruto

PKI
Infraestructura pública clave

POTOMAC
Instituto Potomac de Estudios Políticos

REMJA/OEA
Reuniones de Ministros de Justicia o Fiscales Generales de las Américas

SCADA
Control de Supervisión y Adquisición de Datos

SEI
Software Engineering Institute (de Carnegie Mellon University)

SENATICS
Secretaría Nacional de Tecnologías de Información y Comunicaciones (Paraguay)

SUSCERTE
Superintendencia de Servicios de Certificación Electrónica (Venezuela)

TCBM
Medidas de transparencia y de fomento de la confianza

TI
Tecnología de la información

TIC
Tecnología de la información y la comunicación

UIT
Unión Internacional de Telecomunicaciones

UIT-IMPACT
Alianza Internacional y Multilateral contra las Amenazas Cibernéticas de la UIT

WEF
Foro Económico Mundial

Si los lectores han de llevarse un sólo mensaje de este Informe 2016 del Observatorio de la Ciberseguridad en América Latina y el Caribe, es que una enorme mayoría de nuestros países aún están poco preparados para contrarrestar la amenaza del cibercrimen. Su análisis es un llamado a la acción para empezar a hacer todo lo necesario por proteger esta infraestructura clave para el siglo XXI.

Hay mucho en juego. Según algunos cálculos, el cibercrimen le cuesta al mundo hasta US$575.000 millones al año[1], lo que representa 0,5% del PIB global. Eso es casi cuatro veces más que el monto anual de las donaciones para el desarrollo internacional. En América Latina y el Caribe, este tipo de delitos nos cuestan alrededor de US$90.000 millones al año[2]. Con esos recursos podríamos cuadruplicar el número de investigadores científicos en nuestra región.

Las ventajas de la conectividad son innegables, y los latinoamericanos y caribeños adoptan estas nuevas tecnologías con entusiasmo. Hoy somos el cuarto mayor mercado móvil del mundo, la mitad de nuestra población usa el Internet y nuestros gobiernos emplean cada vez más medios digitales para comunicarse y brindar servicios a los ciudadanos.

Pero en donde nos quedamos cortos es en prevenir y mitigar los riesgos de la actividad delictiva o maliciosa en el ciberespacio. El Modelo de Madurez de Capacidad de Seguridad Cibernética desarrollado en este informe es un buen punto de referencia para comenzar a encontrar soluciones que permitan remediar esta situación.

Un análisis de sus 49 indicadores demuestra que muchos países de la región son vulnerables a ataques cibernéticos potencialmente devastadores. Cuatro de cada cinco países no tienen estrategias de ciberseguridad o planes de protección de infraestructura crítica. Dos de cada tres no cuentan con un centro de comando y control de seguridad cibernética. La gran mayoría de las fiscalías carece de capacidad para perseguir los delitos cibernéticos.

Si vamos a sacarle la mayor ventaja posible a la llamada cuarta revolución industrial[3], tenemos que crear una infraestructura digital no sólo moderna y robusta sino también segura. Proteger a nuestros ciudadanos del cibercrimen no es una mera opción: es un elemento clave para nuestro desarrollo.

Como tantos de los desafíos que enfrentamos en pos de ese desarrollo, este es un reto que excede la capacidad de cualquier institución. Nuestros esfuerzos individuales se potencian cuando trabajamos con aliados que comparten nuestros objetivos y valores. Este informe se benefició de ese tipo de colaboración gracias a los aportes de la Organización de los Estados Americanos, la Universidad de Oxford, el Center for Strategic International Studies, la Fundación Getúlio Vargas, la organización FIRST, el Consejo de Europa, Potomac Institute y el Foro Económico Mundial.

Espero que esta evaluación rigurosa y sistemática, con sus útiles indicadores, sirva de guía y aliciente a los responsables de la ciberseguridad de nuestra región para avanzar rápidamente en el camino correcto. Quienes medran con el cibercrimen no nos darán tregua.

Luis Alberto Moreno
Presidente
Banco Interamericano de Desarrollo

Notas

1. Center for Strategic and International Studies and McAfee (Firm). *Net Losses : Estimating the Global Cost of Cybercrime*. P.23, 2014. Web.

2. Prandini, Patricia y Marcia L. Maggiore. *Panorama del ciberdelito en Latinoamérica.* Documento de trabajo. Montevideo: Registro de Direcciones de Internet para Latinoamérica, 2011.

3. El Professor Klaus Schwab, Director Ejecutivo y Fundador del Foro Económico Mundial, definió el concepto de la Cuarta Revolución Industrial mismo que guío la agenda de la última Reunión Anual en Davos en Enero del 2016. http://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond.

Organization of
American States
More rights for more people

La realidad contundente de nuestro tiempo es que el Internet ha revolucionado la forma en que interactuamos con los demás y el mundo que nos rodea. El aumento de la conectividad a Internet hace que un número cada vez mayor de personas estén conectadas en un espacio en gran parte público y transnacional, y proporciona una plataforma dinámica y de crecimiento que permite que avance la comunicación, la colaboración y la innovación en maneras en que nunca hubiéramos podido imaginar hace muy poco tiempo. Esto es particularmente cierto en América Latina y el Caribe, donde más de la mitad de nuestra población ya está en línea y la tasa de crecimiento de usuarios de Internet se encuentra entre las más altas del mundo. En las Américas y el Caribe estamos utilizando el Internet para compartir ideas y cultura; para mejorar el gobierno y los servicios sociales; para colaborar en la educación, las ciencias y las artes; y para hacer negocios, todo con una mayor accesibilidad y eficiencia. Los mayores beneficios de este nuevo paradigma que está emergiendo rápidamente es el impacto que ha tenido en la estimulación de un nuevo crecimiento y desarrollo social y económico de la región.

No se puede ignorar, sin embargo, que nuestra creciente conectividad y dependencia de las plataformas y servicios basados en Internet han aumentado considerablemente nuestra exposición al riesgo -la de nuestros ciudadanos, empresas comerciales y gobiernos- a una gran cantidad de actividades y actores relacionados con la delincuencia y seguridad. Los datos disponibles indican claramente que los incidentes y ataques cibernéticos, en particular los que se realizan con intención criminal, están aumentando en frecuencia y sofisticación. Las agencias gubernamentales y las empresas han llegado a reconocer la necesidad de tener fuertes marcos, medidas y capacidades de seguridad cibernética, así como contar imperiosamente con cooperación e intercambio de información. En la actualidad se entiende que el delito cibernético no reconoce fronteras nacionales y que se requiere un esfuerzo multilateral y multidimensional para abordar la cantidad de amenazas informáticas. De hecho, se está avanzando de manera importante.

La Organización de los Estados Americanos (OEA) ha estado comprometida principalmente con temas de seguridad cibernética y delincuencia cibernética por más de una década, fomentando y apoyando la labor de nuestros Estados Miembros para fortalecer su capacidad para proteger a las personas, las economías y la infraestructura crítica de nuestra región contra la delincuencia cibernética y otros ataques o incidentes cibernéticos. En 2004 los Estados Miembros de la OEA aprobaron la Estrategia Interamericana Integral para Combatir las Amenazas a la Seguridad Cibernética, que abogaba por un esfuerzo coordinado de múltiples partes interesadas en la lucha contra las amenazas cibernéticas en el hemisferio y proporcionaba un marco inicial para cultivar y guiar tal enfoque. Nuestros Estados Miembros fueron extraordinariamente previsivos cuando adoptaron esta visión desde el principio. Al hacerlo, creamos un espacio en el que la cooperación significativa, entre un amplio número de partes interesadas, ha mejorado el intercambio de información, mejorado la protección de la infraestructura de las tecnologías de la información y las comunicaciones (TIC), fortalecido la capacidad de nuestros gobiernos para responder y mitigar incidentes cibernéticos y reforzado nuestra resiliencia individual y colectiva frente a amenazas cibernéticas. Estos compromisos se han reafirmado y fortalecido con los años, a partir de la adopción de numerosas declaraciones oficiales, incluyendo uno recientemente, en marzo de este año, en relación con el papel y las responsabilidades de la OEA y sus Estados Miembros en la promoción de la seguridad cibernética, la lucha contra la delincuencia informática y la protección de infraestructuras de información crítica.

El Programa de Seguridad Cibernética del Comité Interamericano contra el Terrorismo de la OEA (CICTE) ha jugado un papel clave en este frente. El programa ha ayudado a Estados Miembros a elaborar estrategias de seguridad cibernética nacional, ha brindado capacitación a los Equipos de Respuesta a Incidentes de Seguridad Informática (CSIRT) nacionales y regionales, ha facilitado ejercicios de gestión de crisis con operadores de la industria nacional crítica y los activos de respuesta a emergencias, la sociedad civil dedicada y el sector privado y ha ayudado a crear conciencia sobre las amenazas y las oportunidades relacionadas con la seguridad cibernética en nuestra región. En estas y otras maneras, el CICTE ha contribuido directamente a contar con un dominio cibernético más seguro y vigilante en el Caribe y América Latina.

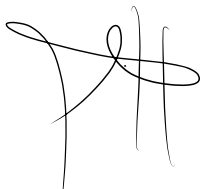
A pesar de los avances prometedores que hemos logrado hasta el momento, la necesidad de continuar con cooperación multilateral y la creación de capacidad sigue siendo igual de urgente. Las tecnologías de la información y las innumerables formas en que las utilizamos siguen evolucionando a un ritmo acelerado, al igual que las vulnerabilidades que traen consigo y los actores y las amenazas que buscan aprovecharse de estas. Solo trabajando juntos podemos seguir el ritmo y asegurar que los beneficios de este dominio digital nuevo y en expansión supere los riesgos y los costos.

Esto requiere que cultivemos una comprensión de todo el alcance de las amenazas a nuestro dominio cibernético, basado en la más completa y actualizada información disponible. Sin embargo, hay una escasez de literatura integral en materia de seguridad cibernética en América Latina y el Caribe. Desde 2013, el Programa de Seguridad Cibernética del CICTE de la OEA ha tratado de abordar este vacío de información a través de una serie de informes integrales, preparados y publicados en colaboración con líderes de la industria de seguridad cibernética. Estos informes han sido muy explicativos, ofreciendo la imagen más detallada y precisa a la fecha de la seguridad cibernética y la delincuencia cibernética en nuestro hemisferio.

Siguiendo con esta tradición, la OEA se complace en presentarles, en colaboración con el Banco Interamericano de Desarrollo (BID) y el Centro Global de Seguridad Cibernética de la Universidad de Oxford, el Observatorio de Seguridad Cibernética en América Latina y el Caribe.

Este estudio tiene como objetivo profundizar en el conocimiento de los riesgos de seguridad cibernética, los retos y oportunidades en América Latina y el Caribe. Mediante la utilización de encuestas y otros datos aportados por expertos y funcionarios de treinta y dos Estados Miembros de la OEA, el informe examina la "madurez cibernética" de cada país en cinco dimensiones: 1) política y estrategia de seguridad cibernética; 2) cultura y sociedad cibernética; 3) educación, formación y competencias en seguridad cibernética; 4) marcos jurídicos y reglamentarios; y 5) normas, organizaciones y tecnologías. También hay que señalar que el Programa de Seguridad Cibernética de la OEA recibió generoso apoyo de Microsoft, que ayudó a identificar áreas clave que se presentaran en la fase inicial del proyecto. El enfoque del informe de país por país deberá ayudarnos a desarrollar una comprensión más sutil de cada uno de los regímenes de seguridad cibernética de nuestros Estados y ayudar a los responsables políticos y técnicos tanto a mejorar estratégicamente los esfuerzos existentes de seguridad cibernética como a diseñar e implementar nuevas iniciativas en el futuro.

Hay que reconocer que estos resultados solo representan una instantánea en el tiempo de un paisaje siempre cambiante. Se necesitarán más estudios para continuar al tanto de la situación de la seguridad cibernética en las Américas y el Caribe. Sin embargo, esperamos que al mejorar nuestra comprensión colectiva de los retos y oportunidades de seguridad cibernética que enfrenta actualmente nuestra región, la información y análisis contenidos en este informe ayudarán a los interesados en todos los sectores –gobierno, sector privado, academia y sociedad civil– a trabajar mejor juntos para construir un ciberespacio más seguro, resiliente y productivo en nuestro hemisferio. Confiamos en poder seguir desempeñando un papel en esta misión vital.



Luis Almagro
Secretario General
Organización de los Estados Americanos

Sobre este informe

El Informe 2016 del Observatorio de la Ciberseguridad en América Latina y el Caribe es el resultado de una gestión de colaboración entre el Banco Interamericano de Desarrollo (BID) y la Organización de los Estados Americanos (OEA) para presentar una imagen completa y actualizada del estado de la seguridad cibernética de los países de América Latina y el Caribe. El uso de una herramienta en línea diseñada en conjunto con el Centro Global de Capacidad sobre Seguridad Cibernética de la Universidad de Oxford facilitó la recolección de datos por parte de la OEA-BID de los interesados en seguridad cibernética que representan distintos sectores. Estos interesados incluyen: agencias gubernamentales, operadores de infraestructuras críticas, las fuerzas militares, la policía, el sector privado, la sociedad civil y la academia. Se consiguió información adicional a través de diversas fuentes secundarias, que se ha citado a lo largo del informe.

Este informe consta de dos secciones principales. La primera sección, "Contribuciones de expertos", consta de ensayos sobre las tendencias de la seguridad cibernética en la región, aportados por expertos internacionales en seguridad cibernética. James A. Lewis, del Centro de Estudios Estratégicos e Internacionales (CSIS), explora el papel de la cooperación internacional en la creación y regulación normativa para la seguridad cibernética y delincuencia cibernética en "Fomento de confianza cibernética y diplomacia en América Latina y el Caribe". Lewis destaca el trabajo de los mecanismos regionales e internacionales para promover la cooperación internacional en la protección del ciberespacio. En "Seguridad cibernética, privacidad y confianza: tendencias en América Latina y el Caribe. El camino a seguir", Marília Maciel, Nathalia Foditsch, Luca Belli y Nicolás Castellón del Centro de Tecnología y Sociedad (CTS) de la Fundación Getúlio Vargas (FGV) analizan el desafío de equilibrar el intercambio de información con la privacidad y la libertad de expresión y señalan la importancia de contar con medidas tales como los marcos regulatorios de privacidad y protección de datos y plataformas de múltiples partes interesadas, entre otros. En el siguiente segmento, Maarten Van Horenbeeck, Cristine Hoepers y Pete Allor del Foro de Equipos de Respuesta a Incidentes de Seguridad (FIRST) escriben sobre la necesidad de contar con capacitación y oportunidades educativas para los Equipos de Respuesta a Incidentes de Seguridad Informática (CSIRT), así como una "comunidad fuerte e incluyente de CSIRT". Luego, Alexander Seger del Consejo de Europa (CoE) examina cómo los países de América Latina y el Caribe han diseñado y actualizado sus marcos legislativos para abordar los delitos informáticos, con especial énfasis en la Convención de Budapest y presenta una serie de estudios de caso. En "Economía digital y seguridad cibernética en América Latina y el Caribe", el Consejo de la Agenda Global sobre Seguridad Cibernética del Foro Económico Mundial (WEF) analiza las conexiones entre el desarrollo de las TIC, la seguridad cibernética y las economías nacionales de América Latina y el Caribe. Por último, Melissa Hathaway y Francesca Spidalieri del Instituto Potomac opinan sobre lo esenciales que son la sostenibilidad y seguridad para asegurar la viabilidad económica a largo plazo de la innovación y el crecimiento de las TIC.

La segunda sección, "Reporte de países" presenta una visión general del estado actual de la seguridad cibernética en los países de la región del Caribe y América Latina sobre la base de la información obtenida a través de la herramienta en línea diseñada en colaboración con el GCSCC, de entrevistas con funcionarios de los Estados Miembros y la investigación documental. Los datos recogidos fueron analizados mediante el uso de los 49 indicadores del modelo de madurez de la capacidad de seguridad cibernética desarrollado por el GCSCC, que se divide en cinco dimensiones: 1) Política; 2) Sociedad; 3) Educación; 4) Legislación; y 5) Tecnología. Hay cinco niveles de madurez para cada indicador: 1) Inicial; 2) Formativo; 3) Establecido; 4) Estratégico; y 5) Dinámico. La profesora Sadie Creese, del GCSCC de la Universidad de Oxford, introduce los reportes de países y da su puntos de vista sobre las conclusiones y algunas de las tendencias regionales que sugieren. Cada perfil de país ofrece una breve reseña de los acontecimientos recientes de seguridad cibernética en el país, las estadísticas sobre la población del país, el número de personas con acceso a Internet, las suscripciones de telefonía móvil y el porcentaje de penetración de Internet. Además, cada perfil muestra el nivel de madurez del país para cada indicador.

A raíz de los informes de país, Melissa Hathaway, Jennifer McArdle y Francesca Spidalieri del Instituto Potomac de Estudios Políticos ofrecen sus puntos de vista sobre las conclusiones de los informes. Señalan el creciente compromiso y la inversión que la región de ALC ha puesto a la seguridad cibernética, al tiempo que reconocen los desafíos pendientes, incluyendo las necesidades para las estrategias nacionales de seguridad cibernética, una mayor conciencia social de los riesgos cibernéticos, las asociaciones público-privadas y los mecanismos de intercambio de información.

Este informe procura presentar una representación integral de la ciberseguridad en la región. Las partes interesadas nacionales de diversos sectores pueden utilizar esta información para comprender mejor la situación de la seguridad cibernética de su país en un contexto regional. Ello también puede ayudarles a los gobiernos y expertos en seguridad cibernética a explorar nuevas ideas para el fortalecimiento de la seguridad cibernética en sus respectivos países y en todo el hemisferio. En general, los resultados representan una instantánea en el tiempo, que se puede utilizar como punto de referencia a medida que los países continúen desarrollando sus capacidades de ciberseguridad.

Contribuciones de expertos

Fomento de confianza cibernética y diplomacia en América Latina y el Caribe

CSIS | **Centro de Estudios Estratégicos e Internacionales**
James A. Lewis

La conectividad a Internet acelera el crecimiento económico y crea oportunidades para los negocios y el comercio. La maximización del valor de la Internet y el ciberespacio debe ser una parte central de la planeación gubernamental. Sin embargo, estas oportunidades siempre traen sus riesgos. Las tecnologías de Internet aún no están maduras. Los delincuentes las pueden explotar fácilmente. Este riesgo es manejable, pero requiere de la atención de los líderes nacionales. Para que el tema de la seguridad cibernética llegue al nivel más alto del liderazgo político, todavía depende de varios factores: el interés personal, haber experimentado directamente la acción cibernética maliciosa y las relaciones con otros Estados. Sin embargo, un número creciente de presidentes y primeros ministros de todo el mundo han convertido la seguridad cibernética en una prioridad.

Se ha generado un amplio debate internacional sobre la seguridad cibernética en los últimos años, lo que refleja el deseo de las naciones de responder a las tendencias inquietantes y de reforzar la estabilidad y la seguridad de los recursos mundiales cibernéticos. La comunidad internacional se ha centrado en los temas de las normas de seguridad cibernética, las medidas de generación de confianza y la creación de capacidades.

Esta es la agenda internacional para la seguridad cibernética y merecen especial atención cuatro grupos de discusión. Se trata de las conversaciones en el Grupo de Expertos Gubernamentales de las Naciones Unidas (GEG), la Organización para la Seguridad y la Cooperación en Europa (OSCE), el Foro Regional de la Asociación de Naciones del Sureste Asiático (ASEAN, por sus siglas en inglés), y la OEA. También es digno de mención el papel de liderazgo del Proceso de Londres, puesto en marcha en 2011 por el entonces secretario de Relaciones Exteriores del Reino Unido, William Hague. Esta serie de reuniones internacionales informales tienen como objetivo generar un consenso sobre un comportamiento responsable en el ciberespacio. Ha habido cuatro reuniones, la última de las cuales, realizada en La Haya, elaboró un Informe del Presidente muy completo que recomienda una serie de posibles normas y estableció el "Foro Mundial sobre Experticia Cibernética". La OEA es miembro fundador de este último. El Foro facilitará el intercambio de experiencias, conocimientos y buenas prácticas entre los responsables políticos y expertos cibernéticos de diferentes países y regiones. La próxima reunión del Proceso de Londres está programada tentativamente para la primavera de 2017 en el Hemisferio Occidental.

Los GEG han sido de suma importancia para el establecimiento de la agenda global. Se han realizado cuatro en la última década. El tercer grupo de expertos gubernamentales en 2013 fue un éxito inesperado y definió un cambio histórico que alteró el panorama político de la Internet. Implicó el reconocimiento de que la soberanía nacional, la Carta de la ONU y el derecho internacional se aplican al ciberespacio, revirtiendo, en pocas palabras, todo el edificio de un "bien común mundial". La Asamblea General de la ONU aprobó esta aplicabilidad de la soberanía, el derecho y la Carta de la ONU, y esto cambió la política de la Internet y su gobernanza y de manera muy provechosa insertó el debate internacional sobre la seguridad cibernética en el marco actual de las obligaciones y el entendimiento entre los Estados.

Hacer frente a estos desafíos requiere de esfuerzos diplomáticos y la cooperación internacional. Algo que hemos aprendido en seguridad cibernética es que ninguna nación por sí sola puede asegurar adecuadamente sus redes. La cooperación es esencial.

El cuarto GEG, que concluyó en junio de 2015, fue presidido por un alto diplomático brasileño y contó con la participación de Colombia, México y Estados Unidos. Se pudo llegar a un consenso (en buena medida debido a la habilidad del Presidente), pero el Informe aún no ha sido aprobado por la Asamblea General. Este Grupo de Expertos Gubernamentales aprobó un conjunto adicional de normas y medidas para desarrollar capacidad y definió una serie de medidas de generación de confianza voluntarias para aumentar la transparencia y fortalecer la cooperación. Sorprendentemente, no fueron las normas las que resultaron ser el tema más polémico, sino más bien la aplicación del derecho internacional para el ciberespacio, un área sobre la cual se necesitará trabajar más en el futuro debate internacional.

En su labor, el Grupo de Expertos Gubernamentales de 2015 se guió por los precedentes creados por un acuerdo de la OSCE en 2014 sobre medidas de fomento de confianza. Después de difíciles negociaciones, la OSCE adoptó un conjunto fundamental e inicial de medidas voluntarias para aumentar la transparencia y la cooperación. Estas medidas de generación de confianza se centran en la transparencia y la coordinación. Entre las medidas voluntarias acordadas en la OSCE se incluyen la provisión de opiniones nacionales sobre la doctrina, estrategia y amenazas

cibernéticas. Los miembros de la OSCE también compartirán información sobre organizaciones, programas o estrategias nacionales pertinentes a la seguridad cibernética, identificarán un punto de contacto para facilitar la comunicación y el diálogo sobre cuestiones de seguridad relacionadas con TIC y establecerán vínculos entre los CERT nacionales.

El trabajo de los Grupos de Expertos Gubernamentales y la OSCE tiene implicaciones útiles para otras regiones del mundo, incluida América Latina y el Caribe, y para seguir avanzando en la construcción de la seguridad cibernética a nivel regional y nacional. La OEA tiene un papel líder a nivel mundial en el desarrollo de la cooperación internacional en materia de seguridad cibernética. Su trabajo sobre el desarrollo de capacidades es un modelo para otras regiones. Ha implementado un número importante de medidas para mejorar la seguridad cibernética en todo el hemisferio. El Comité sobre Seguridad Hemisférica de la OEA publicó una "Lista Consolidada de Medidas de Generación de Confianza y Seguridad" que incluye intercambios voluntarios de información sobre la organización, la estructura, el tamaño de las entidades cibernéticas del gobierno, el intercambio de documentos de política y doctrina, el establecimiento de puntos de contacto nacionales en materia de protección de infraestructuras críticas e intercambio de investigación entre Estados Miembros.

Esta institución también ha organizado una extensa serie de talleres y eventos de capacitación sobre estrategias nacionales, medidas de fomento de confianza y el desarrollo de experticia cibernética. Sus gestiones (ahora con la colaboración del Banco Interamericano de Desarrollo) para vincular la seguridad cibernética a las iniciativas de gobernanza eficaces les ayuda a los Estados Miembros en el trabajo de implementar el gobierno electrónico de forma segura. Una de las áreas a considerar es cómo extender aún más la labor de la OEA y el BID sobre las medidas de generación de confianza de manera que cubra asuntos de seguridad cibernética.

Estos esfuerzos para facilitar el desarrollo de estrategias nacionales y para desarrollar la capacidad han posicionado a las Américas como un líder global en seguridad cibernética. Sin embargo, en América Latina y el Caribe, como en todas las regiones, los esfuerzos para lograr la estabilidad y la seguridad del ciberespacio están en una etapa temprana. Los principales desafíos que enfrenta la región en seguridad cibernética son el desarrollo de capacidades en todos los países, la mejora de la cooperación en delitos cibernéticos y el intercambio de información sobre mejores prácticas, amenazas y vulnerabilidades.

Hacer frente a estos desafíos requiere de esfuerzos diplomáticos y la cooperación internacional. Algo que hemos aprendido en seguridad cibernética es que ninguna nación por sí sola puede asegurar adecuadamente sus redes. La cooperación es esencial. Esto hace que las gestiones regionales sean aún más importantes, especialmente teniendo en cuenta los vínculos entre la seguridad cibernética, el desarrollo y el crecimiento económico. Las economías nacionales que están conectadas a la Internet global y que aprovechan el servicio de Internet crecen más rápidamente y se van enriqueciendo. Una mejor seguridad cibernética les permite a los países aprovechar al máximo estas oportunidades.

Por esta razón, es útil considerar qué medidas adicionales se podrían realizar en el marco de la OEA sobre una base regional, no solo entre los gobiernos sino también entre las comunidades académicas y empresariales. América Latina y el Caribe, sobre la base del trabajo ya realizado, debería centrarse en cuatro pasos.

En primer lugar, la región debería continuar su labor en la creación de una base jurídica armonizada para abordar los delitos cibernéticos. El mejor vehículo para esa cooperación es la Convención de Budapest sobre el delito cibernético, pero hay obstáculos políticos para poder llegar a un acuerdo. Algunos países se oponen a la Convención alegando motivos justificables de que no participaron en la negociación. Estas naciones no se han manifestado acerca de qué cambiarían en la Convención; sin embargo, y vale la pena señalarlo, los países con leyes de delitos cibernéticos débiles sufren mayores pérdidas económicas.

En segundo lugar, sería útil seguir avanzando para llegar a un entendimiento común sobre las infraestructuras críticas y sus vulnerabilidades (una cuestión planteada por el experto colombiano en el GEG), incluyendo una definición compartida de infraestructuras cruciales.

En tercer lugar, sería beneficioso contar con un enfoque regional más formal para la generación de confianza, a partir de la "Lista Consolidada de Medidas de Fomento de Confianza y Seguridad" y basándose en el trabajo de la OSCE. Esto implicaría el intercambio de documentos nacionales de políticas y leyes, reuniones periódicas entre funcionarios relevantes, incluidos los funcionarios a nivel político, para discutir temas de la estabilidad, comercio y seguridad y el fortalecimiento de redes de cooperación de funcionarios responsables a disposición para consulta inmediata o asistencia en caso de una emergencia.

En cuarto lugar, la región se beneficiaría de una formulación continua de estrategias nacionales de seguridad cibernética. Ya ha habido avances en este sentido, pero este progreso no es universal.

El contar con una estrategia aporta cierto grado de organización y coherencia a los esfuerzos nacionales y ofrece transparencia y seguridad tanto para ciudadanos como para países vecinos. El desarrollo de una estrategia es, por supuesto, una prerrogativa nacional, pero hay muchas ventajas en un enfoque de colaboración para el debate y desarrollo de este tipo de estrategias.

Se pueden describir brevemente los elementos generales de una estrategia nacional. Los países necesitan un órgano de coordinación en las oficinas de la Presidencia o del Primer Ministro para supervisar la aplicación, coordinar las gestiones de las entidades y, a veces, resolver disputas. La estrategia debe asignar responsabilidades para la seguridad cibernética entre los ministerios pertinentes y estos ministerios deben desarrollar fuertes lazos con el sector privado para crear un enfoque de colaboración, en particular con la energía eléctrica, las telecomunicaciones y las finanzas. Los gobiernos nacionales necesitan organizaciones de seguridad cibernética adecuadamente atendida que incluyan como mínimo un CERT nacional y policía cibernéticamente capaz. Por último, debe haber un esfuerzo para generar la confianza y relaciones de cooperación con los países vecinos y que contribuya al esfuerzo global para hacer que el ciberespacio sea más seguro. La creación de capacidad sigue siendo esencial y todas las naciones se benefician del intercambio de mejores prácticas y de información sobre amenazas y vulnerabilidades. Tener una estrategia nacional es esencial para la generación de confianza y seguridad entre las naciones de la región.

Ha habido un buen avance, pero los gobiernos ignoran la seguridad cibernética, lo cual es muy riesgoso. A medida que todas las sociedades se vuelvan más dependientes de las máquinas y las redes soportadas por computadores (y esto es inevitable ya que las computadoras están incrustadas en los objetos de uso cotidiano, tanto en los automóviles como en maquinaria industrial), la necesidad de adelantar acciones crecerá. En esto, el Hemisferio Occidental ha avanzado mucho, pero aún queda mucho trabajo por hacer. ■

James Andrew Lewis

Director y Miembro Senior, Programa Estratégico de Tecnologías

Centro de Estudios Estratégicos e Internacionales

James Andrew Lewis es miembro senior y director de programa del Centro de Estudios Estratégicos e Internacionales (CSIS). Antes de vincularse a CSIS, trabajó en los Departamentos de Estado y Comercio como oficial del Servicio Exterior y como miembro del Servicio Ejecutivo Senior. Su experiencia en el gobierno incluye el trabajo en temas político-militares de Asia, como negociador en materia de armas convencionales y transferencia de tecnología, y sobre tecnologías militar y de inteligencia. Lewis encabezó la delegación de Estados Unidos al Grupo de Expertos del Arreglo de Wassenaar en tecnologías civiles y militares avanzadas y fue el ponente del Grupo de Expertos Gubernamentales de las Naciones Unidas en Seguridad de la Información en sus exitosas sesiones de 2010 y 2013. Fue asignado al Comando Sur de los Estados Unidos para la Operación Causa Justa, el Comando Central de Estados Unidos para la Operación Escudo del Desierto, y a la Fuerza Especial de Centroamérica de Estados Unidos. Desde que llegó al CSIS, Lewis ha escrito numerosas publicaciones. Su trabajo más reciente se centra en la seguridad cibernética, incluyendo el *best-seller* "Seguridad cibernética para la 44a Presidencia", que fue elogiado por el presidente Obama. Lewis recibió su Ph.D. de la Universidad de Chicago.

CSIS | Centro de Estudios Estratégicos e Internacionales
www.csis.org
contact@csis.com

Seguridad cibernética, privacidad y confianza: tendencias en América Latina y el Caribe. El camino a seguir

FGV | **Fundación Getúlio Vargas**
Marília Maciel, Nathalia Foditsch, Luca Belli y Nicolás Castellón

Introducción: cuestiones fundamentales en juego

Los objetivos de las estrategias de seguridad cibernética son por lo general dos: i) proteger a la sociedad frente a las amenazas cibernéticas; y ii) fomentar la prosperidad económica y social en un contexto en el que las principales actividades se basan en el uso de Tecnologías de la Información y de la Comunicación (TIC). Con el fin de alcanzar plenamente estos objetivos, las estrategias de seguridad cibernética nacional deben armonizarse con los valores y derechos fundamentales, tales como la privacidad, la libertad de expresión y el debido proceso, así como con los principios técnicos clave que han permitido la innovación en Internet, tales como la apertura, la universalidad y la interoperabilidad[1]. El respeto de los derechos humanos y de estos principios arquitectónicos es clave para fortalecer la confianza y fomentar el crecimiento económico.

El respeto de los derechos humanos y de estos principios arquitectónicos es clave para fortalecer la confianza y fomentar el crecimiento económico.

En las regiones desarrolladas del mundo, las estrategias de seguridad cibernética tienen un enfoque integral, que abarca aspectos económicos, sociales, educativos, jurídicos, de aplicación de la ley, técnicos, diplomáticos, militares y relacionados con la inteligencia[2]. Las consideraciones de soberanía en la formulación de políticas de seguridad cibernética son cada vez más relevantes y se puede notar una mayor participación de los militares y de las ramas de inteligencia del gobierno[3]. Sin embargo, cuando las estrategias de seguridad cibernética se centran exclusivamente en asuntos militares y de inteligencia, es posible que no alcancen un equilibrio adecuado entre la seguridad y los derechos, tales como la privacidad y la libertad de expresión y de asociación.

Cuantos más datos se intercambian con el uso de las TIC, más surgen preocupaciones de seguridad y privacidad cibernéticas. Por otra parte, la tendencia cada vez mayor de tener requisitos de retención de datos obligatorios que se justifican en virtud de razones de seguridad puede entrar en conflicto con la privacidad, el anonimato y la libertad de expresión, si los límites de retención de datos y el uso de los datos conservados no se basan en principios, como la necesidad, proporcionalidad y el debido proceso.

Tendencias a nivel de América Latina y el Caribe

La conciencia de la importancia de desarrollar estrategias de seguridad cibernética está aumentando entre los países de la región de América Latina y del Caribe (ALC). Algunos de ellos ya tienen una estrategia en operación, como Colombia, Jamaica, Panamá y Trinidad y Tobago. Otros países están en proceso de su desarrollo, como Costa Rica, Dominica, Perú, Paraguay y Suriname. El nivel de madurez de estas estrategias varía, incluso en términos de proporcionar un marco para la cooperación entre los organismos gubernamentales y con actores externos.

En la región de ALC, el ejército y las entidades de seguridad nacional no han sido ampliamente establecidos como coordinadores del desarrollo de la política de seguridad cibernética. Esto proporciona una ventana de oportunidad positiva para desarrollar políticas de seguridad cibernética en plataformas de múltiples partes interesadas, incluidas las diferentes ramas gubernamentales, la academia, la comunidad

técnica, la sociedad civil y el sector privado. Los países de ALC podrían avanzar hacia un nuevo concepto de seguridad cibernética que no se deriva solamente de los dominios militares y de defensa, sino también de los derechos humanos.

La cooperación entre múltiples interesados es notable en muchos países de ALC. Se puede encontrar, por ejemplo, en la creación de Equipos de Respuesta a Incidentes de Seguridad Informática (CSIRT), que se han generalizado en toda la región. La colaboración entre los CSIRT nacionales ha permitido el intercambio de conocimientos y buenas prácticas, lo que ha llevado a la creación de sistemas de comunicación más seguros y robustos. La mejora de las capacidades nacionales es importante para aumentar la confianza en los servicios digitales públicos y privados, que allanan el camino para una economía digital emergente y la gobernanza electrónica fiable.

También es necesario equilibrar los costos y los beneficios de contar con disposiciones de retención de datos.

Una de las principales preocupaciones planteadas en los países de ALC ha sido la definición y penalización de los delitos cibernéticos[4], ya sea por la creación de nuevas leyes o actualización de las ya existentes. Brasil ofrece un caso interesante. Un proyecto de ley draconiana que contiene disposiciones de delincuencia cibernética se propuso ante el Congreso[5] y tuvo una fuerte oposición por parte de los académicos y la sociedad civil. El gobierno estaba convencido de que, en lugar de una ley penal, Brasil necesitaba definir los derechos y responsabilidades de los usuarios de Internet. Esto culminó en la aprobación del Marco Civil de Internet, que trata temas como la protección de los derechos fundamentales en línea, la neutralidad de la red, la responsabilidad de los intermediarios, las responsabilidades del sector público y la retención de datos.

Otra tendencia regulatoria en la región de ALC es una creciente preocupación por la protección de la privacidad en línea y los datos personales. Después de las revelaciones de Snowden, en 2013, la conciencia de la intersección entre la seguridad cibernética y los datos personales ha quedado más clara, ya que se trataba de comunicaciones electrónicas diarias. A medida que Internet se ha vuelto esencial para el desarrollo socioeconómico de América Latina, las consecuencias de no protegerla puede afectar la confianza de las actividades en línea, que tiene consecuencias potencialmente negativas para la economía de Internet y en la sociedad en su conjunto.

En su estudio de 2014 titulado, "América Latina y la protección de datos personales: hechos y cifras (1985-2014)", Nelson Remolina Angarita encontró que el 70% de los países de América Latina tienen algún tipo de protección de datos en sus constituciones[6]. Por otra parte, distintos países, por ejemplo, Antigua y Barbuda, Argentina, Colombia, Costa Rica, México, Perú y Uruguay, ya han promulgado leyes de protección de datos y otros, como Brasil[7], están en proceso de redacción de estas. A pesar de esto, la retención de los datos obligatorios es una práctica cada vez más utilizada en la región y, en muchos casos, se pueden obtener datos almacenados sin una orden judicial.

La retención de datos puede ser necesaria en algunos casos para reunir pruebas y para permitir que se realice la investigación de delitos cibernéticos. Sin embargo, la recolección de datos personales con fines de investigación debe limitarse a lo estrictamente necesario para la prevención de un peligro real o para la supresión de un delito específico[8]. Por lo tanto, la recopilación de datos en gran volumen es contraria a esta disposición. Aunque las legislaciones nacionales regulan aún más los casos especiales, esto se debe hacer de una manera que no menoscabe estos principios básicos. El procesamiento de la información también debe ser adecuado, pertinente y no excesivo en relación con el propósito para el que fue almacenada[9]. Si no se establecen límites para la retención de datos, se seguirán reduciendo las reglas de privacidad y esto puede poner en grave peligro los derechos fundamentales de los usuarios de Internet. Por otra parte, esto podría representar una carga regulatoria costosa para las empresas, especialmente las pequeñas y medianas. Los siguientes son algunos ejemplos de cómo se aplican estas disposiciones en la región.

En **Argentina**, una ley[10] fue impugnada ante la Corte Suprema, debido a que autorizó la interceptación de teléfonos y comunicaciones electrónicas sin contar con directrices para la aplicación de las disposiciones[11]. Además, se requiere que los datos se almacenen durante 10 años. La ley fue declarada inconstitucional por la Corte Suprema en 2009.

En **Brasil**, el Marco Civil de Internet[12], promulgado en 2014, ha sido considerado como un documento de avanzada que protege los intereses de los ciudadanos. No obstante, sus disposiciones relativas a la retención obligatoria de datos posiblemente podrían inclinar la balanza hacia las preocupaciones de seguridad sobre la privacidad y las libertades civiles. Según el Marco Civil, los

registros de servicios y aplicaciones deben ser almacenados durante seis meses, mientras que los registros de conexión deben almacenarse durante un año[13].

En **México**, se promulgó en 2014 una ley de telecomunicaciones[14] con diferentes disposiciones de retención de datos. Las autoridades públicas pueden acceder a datos retenidos sin una orden judicial. Por otra parte, algunos datos deben almacenarse 24 meses. Esto corresponde a un aumento de 12 meses en comparación con la norma que ya operaba.

Es importante crear canales para una cooperación a varios niveles entre los gobiernos nacionales y las organizaciones internacionales regionales y mundiales que trabajan en el campo.

En **Paraguay**, un proyecto de ley conocido como "pyraweb"[15] requiere proveedores de servicios de Internet para almacenar los metadatos de un año[16]. Por otra parte, las autoridades públicas no necesitaban una orden judicial para solicitar los datos. Después de enfrentarse a la presión política de los grupos de la sociedad civil, el proyecto de ley fue rechazado por el Senado.

El camino a seguir

Teniendo en cuenta las tendencias descritas en este documento, así como la necesidad de proteger el pleno disfrute de los derechos humanos de los usuarios de Internet, se pueden hacer algunas recomendaciones. Estas recomendaciones no abarcan la amplia gama de cuestiones relacionadas con el equilibrio entre la seguridad y la protección de los derechos humanos. Sin embargo, se abordan algunos puntos fundamentales a tener en cuenta por los países dispuestos a salvaguardar los derechos, mientras abordan problemas de seguridad importantes.

Definir y hacer cumplir los marcos regulatorios de protección de datos y privacidad acertados

Es esencial equilibrar la provisión de seguridad con la necesidad de salvaguardar adecuadamente los derechos de los individuos. La aprobación y aplicación de los marcos de privacidad y protección de datos acertados ayudan a lograr este objetivo. También es necesario equilibrar los costos y los beneficios de contar con disposiciones de retención de datos. Mientras que grupos de la sociedad civil están preocupados por cuestiones de privacidad, la industria se preocupa por la carga normativa que tiene que enfrentar, lo que se traduce en mayores costos para operar sus negocios. Deben utilizarse los principios como la necesidad y proporcionalidad para evaluar lo adecuado de estas disposiciones.

La creación de plataformas nacionales multisectoriales sostenibles

Es importante tener en cuenta los diferentes aspectos y consecuencias, así como la viabilidad técnica de la promulgación de nuevas regulaciones. Grupos de la sociedad civil, la academia y la comunidad técnica, así como representantes de la industria pueden proporcionar valiosa experiencia desde sus perspectivas, y ayudar a diseñar un marco reglamentario racional de una manera sostenible. Estas redes de múltiples partes interesadas podrían ayudar a desarrollar un enfoque con visión de futuro para la seguridad cibernética en la región, que tiene en cuenta los avances tecnológicos, como dataficación, grandes datos y la Internet de las cosas, y que tiene en cuenta el impacto de estas tecnologías en la seguridad y privacidad.

Fortalecimiento de la cooperación internacional

La seguridad cibernética se ha ido integrando cada vez más en el plano internacional[17]. Es importante crear canales para una cooperación a varios niveles entre los gobiernos nacionales y las organizaciones internacionales regionales y mundiales que trabajan en el campo. Fortalecer la cooperación regional también puede facilitar la inclusión significativa de los países de la región en las discusiones globales en curso. La naturaleza sin fronteras de Internet aumenta la importancia de la cooperación internacional y la armonización de los marcos legales.

Conclusión

Este documento presenta una breve descripción de cómo los países de América Latina han abordado la interacción entre la seguridad cibernética y los derechos fundamentales, centrándose en particular en el derecho a la privacidad y a la protección de datos personales. También ofrece sugerencias sobre el camino a seguir, tales como el desarrollo de marcos de privacidad y protección de datos adecuados, el fortalecimiento de la cooperación internacional y la creación de marcos claros para la colaboración entre las partes interesadas. Es esencial fomentar el desarrollo de mecanismos de gobernanza democrática apropiados, a nivel nacional e internacional, sobre la base de un esfuerzo multisectorial. ■

Notas

1. DAIGLE, Leslie. "On the Nature of the Internet". Global Commission on Internet Governance Paper series N.7. Marzo de 2015. **https://www.cigionline.org/sites/default/files/gcig_paper_no7.pdf**
2. OECD. "Cyber security policy making at a turning point: Analyzing a new generation of national cybersecurity strategies for the Internet economy". OCDE, 2012, p. 12.
3. Id, p. 14.
4. OAS; Symantec. "Tendencias de Seguridad Cibernética en América Latina y El Caribe, 2014". **http://www.symantec.com/content/es/mx/enterprise/other_resources/b-cyber-security-trends-report-lamc.pdf**
5. Proyecto de Ley 84/99
6. Remolina Angarita, Nelson. Aproximación constitucional de la protección de datos personales en Latinoamérica. Universidad de los Andes, 2014. **http://habeasdatacolombia.uniandes.edu.co/wp-content/uploads/7_-Nelson-Remolina.pdf**
7. Véase **http://participacao.mj.gov.br/dadospessoais/**
8. Consejo de Europa. Comité de Ministros. Recomendación N°R (87) 15 por medio de la cual se regula el uso de los datos personales en el sector de la policía.
9. Consejo de Europa. Convenio para la protección de las personas en relación con tratamiento automático de datos personales. ETS 108, en el artículo 5.
10. Ley 25.873 y Decreto 1563/04.
11. Corte Suprema de la República de Argentina. Halabi, Ernesto c / PEN ley 25.873 y decreto 1563/04 s / amparo. Disponible en **http://defensoria.jusbaires.gov.ar/attachments/1126_escuchas%20telefonicas%20-%20Ley%20Espia.pdf.**
12. Ley 12.965/14.
13. Véanse los artículos 13 a 15 de Ley 12.965/14.
14. Ley de Telecomunicaciones y Radiodifusión, 2014.
15. La palabra "pyraweb" alude a los informantes de los tiempos de la dictadura (pyrague, en guaraní - una lengua indígena).
16. El proyecto de ley se encuentra disponible en **http://odd.senado.gov.py/archivos/file/Proyecto%20de%20Ley8.pdf**
17. La seguridad cibernética es una de las prioridades identificadas en el proceso decenal de examen de los resultados de la Cumbre Mundial sobre la Sociedad de la Información (CMSI). La Visión CMSI + 10 hizo énfasis en la complementariedad entre la seguridad y la privacidad y definió que "la construcción de la confianza y seguridad en la utilización de las TIC, especialmente en temas como la protección de datos personales, la privacidad, la seguridad y la solidez de las redes", debe ser una de las prioridades más allá de 2015. En diciembre de 2013, la Asamblea General de las Naciones Unidas aprobó la resolución 68/167, que expresa su profunda preocupación por el impacto negativo que la vigilancia e interceptación de las comunicaciones pueden tener en los derechos humanos. La Resolución 69/166, aprobada en 2014, se basa en la anterior, pidiendo el acceso a un recurso efectivo para las personas cuyo derecho a la privacidad ha sido violado. El 26 de marzo de 2015, el Consejo de Derechos Humanos creó el mandato de un Relator Especial sobre el Derecho a la Privacidad. Sin embargo, la cooperación intergubernamental en materia de ciberseguridad sigue fragmentada a través de diferentes organismos y foros en las Naciones Unidas. En paralelo, una Conferencia Mundial sobre el Espacio Cibernético (GCCS) anual, conocida como el "Proceso de Londres" ha reunido a los gobiernos y otras partes interesadas para discutir temas en una amplia gama de asuntos relacionados con la seguridad cibernética.

Marília Maciel

Investigadora y coordinadora del Centro de Tecnología y Sociedad de la Escuela de Derecho de la Fundación Getúlio Vargas en Río de Janeiro. Es concejal en la Organización de Apoyo para Nombres Genéricos (GNSO) de la ICANN en representación del Grupo de partes interesadas no comerciales (NCSG). Es miembro de la Junta Consultiva sobre la seguridad en Internet, creado bajo el Comité Gestor de Internet en Brasil. Asimismo, está realizando el doctorado en Relaciones Internacionales de la Pontificia Universidad Católica (PUC de Río de Janeiro).

Nathalia Foditsch

Investigadora en el Centro de Tecnología y Sociedad de la Escuela de Derecho de la Fundación Getúlio Vargas en Río de Janeiro. Ha trabajado para organizaciones internacionales, el Gobierno Federal de Brasil, así como firmas de abogados y grupos de reflexión sobre las leyes de comunicación y asuntos de política. Foditsch es abogada licenciada y tiene título de maestría en Derecho y en Políticas Públicas, ambas de la Universidad Americana.

Luca Belli

Investigador en el Centro de Tecnología y Sociedad de la Escuela de Derecho de la Fundación Getúlio Vargas en Río de Janeiro. Tiene un doctorado en Derecho Público de la Universidad Panthéon Assas (París II) y es fundador y coordinador de la Coalición Dinámica sobre Neutralidad en Internet, así como de la Coalición Dinámica sobre Responsabilidad de la Plataforma, componentes de múltiples partes del Foro de Gobernanza de Internet de las Naciones Unidas.

Nicolás Castellón

Investigador visitante en el Centro de Tecnología y Sociedad de la Escuela de Derecho de la Fundación, en Río de Janeiro. Se especializa en gobernanza de la seguridad cibernética, centrándose en las infraestructuras críticas y usos humanitarios para grandes datos. Tiene una Maestría en Gestión de Crisis y Seguridad de la Facultad de Gobernanza y Asuntos Globales de la Universidad de Leiden.

FGV DIREITO RIO
CENTRO DE TECNOLOGIA E SOCIEDADE

FGV | Fundación Getúlio Vargas
www.portal.fgv.br
marilia.maciel@fgv.br

Creación de la capacidad de respuesta a incidentes en las Américas

FIRST | **Foro de Equipos de Seguridad y de Respuesta a Incidentes**
Maarten Van Horenbeeck, Cristine Hoepers, Pete Allor

Un Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT, por sus siglas en Inglés) se define como un equipo o una entidad dentro de una agencia que proporciona servicios y apoyo a un grupo particular (la comunidad de destino) con el fin de prevenir, manejar y responder a los incidentes de seguridad de la información. Estos equipos están compuestos generalmente por especialistas multidisciplinarios que actúan de acuerdo con los procedimientos y políticas predefinidos para responder rápida y eficazmente a los incidentes de seguridad y para reducir el riesgo de ataques cibernéticos. Hay cientos de CSIRT en el mundo que varían en su misión y alcance. Una de las principales formas de clasificar a los CSIRT es agruparlos por el sector o la comunidad a los que sirven. A continuación se presentan algunos de los CSIRT nacionales dentro de los Estados Miembros de la OEA.

Introducción

El Foro de Equipos de Seguridad y de Respuesta a Incidentes (FIRST) es una asociación mundial de equipos de respuesta a incidentes con miembros en más de 70 países, permitiéndoles responder de manera más eficaz a incidentes de seguridad mediante la provisión de acceso a mejores prácticas, organización de eventos y ofrecimiento de educación para los Equipos de Respuestas a Incidentes de Seguridad Informática (CSIRT, por sus siglas en inglés). Este documento explora algunas de las experiencias que el FIRST ha tenido en la atención a una amplia variedad de circunscripciones, nuestro punto de vista de la capacidad de respuesta a incidentes y lo que las organizaciones pueden hacer para mejorar el estado general de la seguridad cibernética en la región.

Un mundo cada vez más complejo

Cuando se estableció originalmente el FIRST en 1989, el mundo era un lugar muy diferente del actual. En esos primeros años nuestros equipos miembros de respuesta a incidentes ya trataban con incidentes complejos, pero el alcance y la cantidad de los sistemas afectados eran casi globalmente menores, en comparación con el presente. Se comenta que el gusano Morris, que en 1988 comenzó a explorar la creciente red, afectó alrededor del 10% de Internet, o sea, unas 6.000 máquinas en total[1].

Un traslado rápido al presente evidencia un gran número de asuntos complejos, que incluyen:

- Grandes botnets de software malicioso, como Citadel, que Microsoft Corporation estimó haber infectado a más de 1,9 millones de clientes[2].

- Grandes ataques de Denegación de Servicio Distribuido (DDoS) de hasta 500 Gbps[3] que corren el riesgo de afectar los puntos de intercambio de Internet (IXP)[4]. Además, estos ataques DDoS se habilitan a través de una inadecuada configuración de miles de terminales, por lo que el problema se hace imposible de resolver por parte de una sola nación u organización.

- Ataques de código malicioso complejos que aprovechan vulnerabilidades de día cero, apalancadas tanto en ataques muy concretos como en actividades de delincuencia informática.

Estos cambios requieren que se ajusten rápidamente los responsables de las respuestas a incidentes. Los equipos de respuesta a incidentes con responsabilidad nacional cada vez ofrecen una mayor variedad de servicios, incluida la capacidad de proporcionar información fidedigna sobre amenazas de seguridad a las circunscripciones, el trabajo con vendedores y proveedores de servicios para asegurar un ecosistema de Internet más saludable y el tener profundas habilidades de investigación para analizar los ataques que son menos comprendidos. Esto puede ser un gran desafío para los equipos menores de respuesta a incidentes.

Cumplimiento de estos desafíos

Como tal, es importante para la comunidad de respuesta a incidentes reconocer estas diferencias y trabajar sobre las maneras de abordarlas. Dentro del FIRST vemos éxito en estas áreas de la siguiente manera.

- Los Equipos de Respuesta a Incidentes que responden pueden hacer contacto con otros para mitigar ataques.

- Los CSIRT hablan el mismo idioma operativo y tienen expectativas precisas sobre el uso de la información proporcionada cuando trabajan con otro equipo durante un incidente.

- La comunidad cuenta con las herramientas y técnicas que permiten el intercambio automatizado de información. Los analistas aprovechan la información para comprender verdaderamente las ramificaciones del incidente y toman las decisiones acertadas para reducir los riesgos mientras mitigan el ataque.

Para llegar a este punto, vemos necesario el desarrollo de una comunidad de CSIRT fuerte e incluyente, la disponibilidad de formación y educación para los miembros de la comunidad y la necesidad de contar con prácticas estandarizadas dentro de esta comunidad.

La comunidad CSIRT no puede tener éxito en el aislamiento. Uno de los aspectos interesantes de la región de las Américas es que existen grandes discrepancias en el conocimiento de los asuntos de seguridad cibernética entre los países, tanto en el gobierno como en la población general. Se espera que esto continúe a medida que más usuarios nuevos entran en línea y se demuestra en tasas impresionantes de crecimiento de usuarios en todo el continente. Las gestiones en seguridad deben incluir el desarrollo de una cultura de seguridad cibernética, tal como lo propone la OEA[5], lo que crea un ambiente fértil en el que puedan operar los CSIRT.

Las gestiones deben incluir la formación de conciencia de usuarios y operadores de Internet, el fomento de una estrecha colaboración público-privada con el sector privado, y el desarrollo de políticas apropiadas del delito cibernético que apoyen y tengan en cuenta la privacidad. Además la seguridad comienza con la conciencia y el uso de mejores prácticas en tecnología. A este respeto la academia tiene un papel muy importante en la enseñanza a los profesionales no especializados en seguridad sobre cómo construir tecnologías seguras.

Arraigados en la comunidad

Idealmente, la comunidad de CSIRT debería lograr que cada organización cuente con una capacidad de respuesta a incidentes bien equipada. Puede ser un solo individuo o un equipo pequeño, pero cada organización debe poder asumir la responsabilidad por el tráfico que genera. Sin embargo dado el gran número de redes y su respectivo crecimiento, esto podría considerase un panorama ilusorio. Una alternativa es que cada país desarrolle su "CSIRT de último recurso"[6], un CSIRT que puede ser punto de coordinación para aquellas redes que puedan no tener un equipo de respuesta a incidentes bien entrenado y directamente accesible. Se debe entender bien que, al final, cada organización es responsable de su propia seguridad; un equipo nacional solo puede apoyar en la coordinación pero no podrá "desconectar" o investigar cada máquina comprometida.

En 2014, el FIRST y el CERT.br lideraron una iniciativa dentro del Foro de Gobernanza de Internet para el desarrollo de mejores prácticas para la comunidad de los CSIRT. Un aspecto manifestado unánimemente dentro de la comunidad de participantes fue la necesidad de desarrollar un "CSIRT de último recurso" que salga de la comunidad, en lugar de ponerlo en marcha a través de una decisión vertical del gobierno. Para garantizar la efectividad de un CSIRT, la confianza es un requisito muy importante, y la única manera de desarrollar confianza es a través de un historial de colaboración y participación en la comunidad de seguridad. Tiene una importancia menor que el CSIRT sea operado por el gobierno, un proveedor de red, una entidad comercial o la academia, siempre y cuando se desarrolle en asociación con toda la comunidad de trabajo en red y seguridad dentro de la región.

No puede subestimarse la necesidad de contar con CSIRT robustos en empresas, la academia y el gobierno. Los gobiernos tienen un importante papel que desempeñar en motivar el desarrollo de estos equipos, así como percatarse que no pueden "imponer" la confianza que les permita alcanzar sus metas: deben identificar quién les otorga la confianza, fomentar su crecimiento para el país en general y trabajar con todos. La confianza también está ligada a los servicios que un CSIRT ofrece. Cuando un CSIRT se centra correctamente en responder y mitigar un incidente, a menudo las corporaciones y organizaciones extranjeras confiarán más en ellos y proveerán mayor información para apoyar su misión. Esta información puede limitarse cuando el CSIRT cumple un papel en la persecución criminal o es parte de un servicio de inteligencia. El tipo de información proporcionada a cualquiera de estas organizaciones tiende a ser diferente y los roles, por lo tanto, deben segregarse debidamente.

Desarrollo de capacidad

Cuando existe una red de CSIRT, es importante la creación continua de su capacidad. Vemos tres niveles diferentes de mejoramiento en la prestación de servicios de los CSIRT:

Competencia - ¿Puede usted hacerlo? Una competencia define una actividad medible que puede ser desempeñada como parte de las funciones y responsabilidades de una organización. Para el propósito del marco de servicios de los CSIRT, las competencias pueden definirse como los servicios más amplios o como tareas, sub-tareas o funciones necesarias.

Capacidad - ¿Cuánto puede usted hacer? La capacidad define el número de ocurrencias simultáneas de una competencia en particular que una organización puede ejecutar antes de alcanzar alguna forma de agotamiento de recursos.

Madurez - ¿Qué tan bien puede usted hacerlo? La madurez define el grado de eficacia con el que una organización ejecuta una competencia en particular dentro de la misión y las autoridades de la organización.

Es necesario centrarse en cada uno de estos tres elementos a fin de tener éxito en el aumento de la eficacia de un programa de CSIRT.

En 2014 el FIRST lanzó una iniciativa para poner en marcha un programa de educación impulsado por la comunidad[7], el cual se encuentra desarrollando una lista autorizada de los servicios ofrecidos por un CSIRT y pondrá a disposición, sin costo alguno, un currículo detallado para cada servicio. Esta iniciativa es apoyada por varios CSIRT nacionales, incluyendo el CERT.br así como varias organizaciones internacionales, como OEA, y se espera que haga entrega de materiales de formación inicial a finales de 2015.

Normas y estandarización

Un área adicional de inversión para la comunidad de respuesta a incidentes es la estandarización de procedimientos y trabajo en normas abiertas. Hay una necesidad imperiosa de contar con normas que permitan que los equipos de respuesta a incidentes intercambien datos durante un incidente, o lleguen a acuerdos sobre los métodos adecuados para gestionar un determinado tipo de incidente. Las normas les permiten a los equipos aprovechar la confianza que han construido entre ellos y asignar a sus analistas para la solución de problemas difíciles.

Aquí vemos una necesidad de que la comunidad considere la adopción de normas de intercambio de información, tales como STIX ("Structured Threat Information eXpression" en inglés) y TAXII ("Trusted Automated Exchange of Indicator Information" en inglés), así como las normas para definir adecuadamente el riesgo de una vulnerabilidad particular, como el CVSS ("Common Vulnerability Scoring System" en inglés). El FIRST ha apoyado estas y otras normas útiles mediante el patrocinio de su desarrollo[8], como es el caso del CVSS, o el trabajo con nuestros miembros para organizar cursos de formación en la enseñanza de prácticas estandarizadas.

Próximos pasos para la comunidad

Hay mucho trabajo por hacer para garantizar un mayor desarrollo de una Internet segura para los usuarios en las Américas y este trabajo es más importante cada día como consecuencia de las altas tasas de crecimiento en la adopción de Internet. Los gobiernos tienen la oportunidad de motivar al sector privado, la sociedad civil y la academia en el desarrollo de una capacidad de respuesta a incidentes dentro de su sector y dentro de cada una de las organizaciones. Además, los gobiernos deben garantizar que entre los equipos con responsabilidad nacional exista un "CSIRT de último recurso" para su país, que activamente genere confianza con cada una de estas organizaciones y tenga la capacidad, no de decidir en su nombre, sino más bien de coordinar todos los sectores cuando ocurra un incidente.

La OEA desempeña un papel único en su capacidad para convocar a los gobiernos de la región para reunirse y hablar de estos temas. En 2015 el FIRST firmó un Memorando de Entendimiento con la OEA[9], en el que respaldamos el papel importante de la OEA en la ayuda al fortalecimiento de la capacidad de respuesta a incidentes en la región. El FIRST espera poder proporcionarle a la OEA el apoyo de la comunidad técnica y nuestros esfuerzos de educación en el logro de estos objetivos.

Se alienta a las organizaciones que tienen una posición única en la aportación de financiamiento para estos esfuerzos, como el Banco Interamericano de Desarrollo (BID), a que consideren brindar apoyo a estos proyectos de respuesta a incidentes. Al final, los CSIRT limitarán las pérdidas que le causará la delincuencia cibernética a la economía local y pueden ser una fuerza muy importante para el bienestar de una comunidad en desarrollo. Animamos a que estas organizaciones comprendan bien el tipo de servicios que son verdaderamente valiosos, como el apoyo a la capacidad central de respuesta a incidentes, en lugar de respaldar gestiones más costosas y menos eficaces como la vigilancia a gran escala de redes de usuarios finales. El FIRST espera contribuir a estas valoraciones a través de la publicación de nuestra lista de servicios del CSIRT actualizada a finales de 2015.

Conclusión

La comunidad de respuesta a incidentes está experimentando cambios significativos debido a los cambios en los tipos y complejidad de los ataques que necesita combatir. En las Américas, no es muy uniforme la madurez de sus capacidades y hay necesidad de mejoras. Este documento describe una serie de áreas centrales clave para los gobiernos de la región y espera informar cómo se encuentra actualmente la comunidad en el proceso de abordarlas y dónde hay necesidad de asistencia. Identifica cómo los gobiernos pueden beneficiar mejor a la comunidad mediante la identificación de brechas y la motivación de mecanismos existentes para mejorar su competencia o añadir servicios y objetivos adicionales para satisfacer las necesidades de seguridad estratégica de sus economías. ■

Cristine Hoepers

Gerente General de CERT.br, el CERT Nacional brasileño, mantenido por NIC.br, del Comité Gestor de Internet en Brasil. Es graduada en Ciencias de la Computación y tiene un doctorado en Informática Aplicada. Ha estado trabajando con la Gestión de Incidentes en CERT.br desde 1999, donde ayuda en el establecimiento de nuevos CSIRT en el país, ofrece capacitación en seguridad de la información y el manejo de incidentes, y desarrolla mejores prácticas en materia de administración del sistema y sensibilización de los usuarios. Es Presidenta del Grupo de Interés Especial (SIG) Botnet de FIRST y miembro del Consejo Asesor del Proyecto AMPARO de LACNIC. En el pasado se desempeñó como miembro del Comité Directivo de FIRST, miembro del Grupo de Expertos de Alto Nivel de la Unión Internacional de Telecomunicaciones (UIT) y fue uno de los representantes brasileños en la Red Hemisférica de la OEA de CSIRT.

Es profesora autorizada para dictar los cursos del Programa de CERT, del Software Engineering Institute (SEI) de la Universidad Carnegie Mellon y ha participado como conferencista y moderadora en varios foros como la UIT, la OEA, Anti-Phishing Working Group (APWG), Foro para la Gobernanza de Internet (FGI), Plan de Acción de Londres, del Messaging Anti-Abuse Working Group (MAAWG), del Registro de Direcciones de Internet para América Latina y Caribe (LACNIC, por sus siglas en inglés), FIRST y el Equipo de Respuesta ante Emergencias Informáticas de Australia (AusCERT), en temas de manejo de incidentes, fraude por Internet y correo basura, desarrollo de CSIRT y el uso de honeypots para identificar el abuso de la infraestructura de Internet.

Peter Allor

Director en la Junta del FIRST (Foro de Equipos de Respuesta a Incidentes de Seguridad). Ha sido miembro de esta organización mundial de primer nivel y reconocido líder para incidentes desde 2006 y durante los últimos cinco años se desempeñó como Director Financiero y Tesorero, trabajando los aspectos del negocio de FIRST. Org, Inc. Ahora tiene el cargo de Copresidente del Marco de Educación de Servicios CSIRT, impulsando la participación global de los CSIRT nacionales, infraestructuras críticas, empresas y formación no gubernamental o programas universitarios. Trabaja para IBM Security como su jefe estratega de seguridad para gestión de productos y se ocupa de cuestiones de coordinación de divulgación para investigadores IBM X-Force. Es el responsable de la alineación de productos y servicios de IBM para las necesidades del cliente a nivel mundial incluyendo al gobierno, la Internet de las Cosas y SCADA, así como dispositivos médicos. Es miembro del Comité Ejecutivo del Consejo de Coordinación Sectorial de la Tecnología de la Información (IT-SCC), que trabaja en el sector privado en aportes de política y estrategia al Gobierno de Estados Unidos. Es también miembro de la Junta del Consorcio de la Industria para la Promoción de la Seguridad en Internet (ICASI.Org). Es miembro de la norma Inteligencia de la Amenaza cibernética OASIS para actualizar STIX/TAXII y CyBox. También forma parte del Comité de Dirección de la Norma de Ciberseguridad de la Sociedad de Tecnología de la Diabetes para Dispositivos de Diabetes Conectados.

Maarten Van Horenbeeck

Director del Foro de Equipos de Respuesta a Incidentes de Seguridad (FIRST), la principal organización y líder mundial reconocido en respuesta a incidentes. Se ha desempeñado como miembro del Consejo de Administración desde 2011 y fue Presidente de la organización de 2013 hasta 2015. Fuera de su trabajo para FIRST, es Director de Seguridad para Fastly, una red de distribución de contenidos que acelera los sitios web y las API. Tiene 14 años de experiencia profesional en seguridad de la información y ha trabajado en los equipos de seguridad en Amazon, Google y Microsoft. Centró gran parte de su carrera en la creación de programas de respuesta a incidentes e inteligencia de amenazas, especialmente orientados a la investigación y respuesta a los ataques dirigidos. Originario de Bélgica, vive en San Francisco, California, y cuenta con una maestría en Seguridad de la Información de la Universidad Edith Cowan de Australia Occidental.

FIRST | Foro de Equipos de Seguridad y de Respuesta a Incidentes
www.first.org | first-sec@first.org

Notas

1. Denning (1999) en Marchette, David J. "Computer Intrusion Detection and Network Monitoring: A Statistical Viewpoint". New York: Springer-Verlag.

2. Microsoft on the Issues (2013). "Initial revelations and results of the Citadel botnet operation". Consultado el 15 de julio de **http://blogs.microsoft.com/on-the-issues/2013/06/21/initial-revelations-and-results-of-the-citadel-botnet-operation/**.

3. Olson, Parmy (2014). "The Largest Cyber Attack in History Has Been Hitting Hong Kong Sites". New York: Forbes. Consultado el 15 de julio de **http://www.forbes.com/sites/parmyolson/2014/11/20/the-largest-cyber-attack-in-history-has-been-hitting-hong-kong-sites/**.

4. Prince, Matthew (2013). "The DDoS That Almost Broke The Internet". Consultado el 12 de julio de **https://blog.cloudflare.com/the-ddos-that-almost-broke-the-Internet/**.

5. Organización de los Estados Americanos (2014). "A comprehensive Inter-American Cybersecurity strategy: A Multidimensional and Multidisciplinary Approach to Creating a Culture of Cybersecurity". Consultado el 12 de julio de **http://www.oas.org/juridico/english/cyb_pry_strategy.pdf**.

6. Foro de Gobernanza de Internet (2014). "Best Practice Forum on Establishing and Supporting Computer Security Incident Response Teams (CSIRT) for Internet Security". Consultado el 12 de julio de **http://www.intgovforum.org/cms/documents/best-practice-forums/establishing-and-supporting-computer-emergency-response-teams-certs-for-Internet-security/409-bpf-2014-outcome-document-computer-security-incident-response-teams/file**

7. FIRST (2015). FIRST develops framework for education curriculum for global Computer Security Incident Response Teams (CSIRTs). Consultado el 10 de julio de **https://www.first.org/global/education**.

8. FIRST (2015). Common Vulnerability Scoring System v3. Consultado el 16 de julio de **https://www.first.org/cvss**.

9. OEA (2015). OAS and FIRST Sign Agreement to Improve Hemispheric Response to Cyber Incidents. Consultado el 15 de julio de **http://www.oas.org/en/media_center/press_release.asp?sCodigo=E-190/15**.

El estado actual de la legislación sobre el delito cibernético en América Latina y el Caribe: algunas observaciones

CoE | **Consejo de Europa**
Alexander Seger[1]

Marco legal sobre el delito cibernético y la evidencia electrónica: ¿qué se necesita?

La efectividad de la justicia penal es parte esencial de una estrategia de seguridad cibernética. Esto comprende la investigación, la fiscalización y la adjudicación de delitos en contra y por medio de datos y sistemas informáticos, al igual que la obtención de evidencia electrónica relacionada con cualquier delito, para propósitos del proceso penal. La naturaleza transnacional del delito cibernético y en particular la volatilidad de la evidencia electrónica implican que la justicia penal no puede ser efectiva sin una cooperación internacional eficiente.

La legislación integral, que incluye el derecho sustantivo (la conducta a ser definida como delito) y el derecho procesal (los poderes investigativos para la aplicación de la ley), es fundamental para que tenga lugar la respuesta de la justicia penal. Tal legislación debe cumplir con varios requisitos:

- Debe ser lo suficientemente neutral (tecnológicamente) como para responder a la evolución constante del crimen y la tecnología, ya que de no ser así corre el peligro de volverse obsoleta para cuando entre en vigor.
- Los poderes para la aplicación de la ley deben estar sujetos a salvaguardias con el fin de garantizar el cumplimiento de los requerimientos del Estado de derecho y de los derechos humanos.
- Debe operar con suficiente armonía o por lo menos ser compatible con las leyes de otros países para permitir la cooperación internacional; por ejemplo, el cumplimiento con la condición de la doble criminalidad.

A través del Convenio de Budapest sobre el Delito Cibernético[2] existe una directriz internacional, también ampliamente utilizada en las Américas, que ayuda a los países a cumplir estos requerimientos.

En referencia a la ley sustantiva, requiere que las partes penalicen el acceso ilícito, la interceptación ilegal, la interferencia de datos, la interferencia de sistemas, el uso indebido de aparatos, la falsificación informática, el fraude informático, la pornografía infantil y delitos relativos a las infracciones en materia de derechos de autor y derechos relacionados.

Cabe destacar que estas disposiciones por sí solas o en combinación todavía se aplican para la generalidad de lo que constituye el delito cibernético, aún hoy, catorce años después de la adopción del Convenio, dado que han sido formuladas de manera neutral desde el punto de vista tecnológico. Las Notas Guía adoptadas por el Comité del Convenio sobre el Delito Cibernético muestran cómo diversas disposiciones pueden ser utilizadas para tratar con las redes de bots, Ataques Distribuidos de Denegación de Servicios (DDos, por sus siglas en inglés) y otros fenómenos[3].

Por supuesto, un acuerdo internacional siempre representa un mínimo común denominador y los Estados son libres de decidir si van más allá. No obstante, muchos Estados, inclusive en las Américas, a menudo enfrentan oposición pública al tratar de penalizar tipos de conducta adicionales.

El Convenio de Budapest comprende una variedad de poderes específicos de derecho procesal, tales como órdenes para la búsqueda, captura, producción de datos o la interceptación de comunicaciones, así como el poder para ordenar la rápida conservación de datos. Estos se refieren, de manera importante, a la evidencia electrónica asociada con cualquier tipo de delito. Deben ser delimitados bajo condiciones de Estado de derecho y salvaguardia.

Para finalizar, este tratado debe garantizar la efectiva cooperación internacional en materia de delito cibernético y


Política
02/17
***
Legislación
02/17

evidencia electrónica, mediante la combinación de la asistencia legal mutua "tradicional" con medios expeditos para conservar datos en otro país, esto último con el soporte de una red de puntos de contacto que funcione las 24 horas todos los días de la semana. De nuevo, el alcance de la cooperación no se limita al delito cibernético, sino que incluye la cooperación referente a la evidencia electrónica que se halla en un sistema informático a propósito de cualquier delito.

El Convenio de Budapest, por lo tanto, puede servir de lista de verificación para el desarrollo de leyes internas sustantivas y procesales relativas al delito cibernético y la evidencia electrónica. Tal parece que más de 130 Estados en el mundo lo han usado como directriz de una forma u otra. Sin embargo, el Convenio en su totalidad es un documento balanceado, juicioso y coherente y debe considerarse preferiblemente como un todo.

Para los Estados que se convierten en Partes del Convenio, el tratado sirve como un marco legal para la cooperación internacional. El Convenio de Budapest está abierto a la adhesión de cualquier Estado que esté preparado para implementar sus preceptos[4]. En efecto, varios países de América Latina y el Caribe han decidido seguir este camino.

La situación en América Latina y el Caribe

Desde 2004, la OEA –en particular la Reunión de Ministros de Justicia o de Fiscales Generales de las Américas (REMJA/OEA) y su Grupo de Trabajo en Delito Cibernético– ha alentado a sus miembros a implementar los principios del Convenio de Budapest sobre Delito Cibernético y a considerar su adhesión al tratado[5].

Después de la REMJA VI realizada en la República Dominicana en 2006, Costa Rica y México solicitaron ingreso, después de lo cual fueron invitados a acceder al mismo. A partir de entonces, Argentina, Chile, Colombia, Panamá, República Dominicana y recientemente, también Paraguay y Perú han seguido su ejemplo. La República Dominicana y Panamá desde entonces han pasado a formar parte del Convenio de Budapest y se espera que otros países completen con prontitud los procedimientos domésticos de acceso, similares al procedimiento para ratificar cualquier acuerdo internacional.

Este proceso ha sido acompañado de reformas internas en derecho penal. He aquí algunos ejemplos de América Latina.

En 2013, República Dominicana se convirtió en el primer país de América Latina que se adhirió al Convenio de Budapest. La Ley 53-07 de 2007 transpuso las disposiciones del tratado al derecho interno, no solo en lo que respecta a la ley sustantiva, sino también a la ley procesal. Lo anterior es una situación atípica en América Latina, donde se prefiere que los poderes procesales sean aplicados a la evidencia electrónica por analogía[6].

En 2008, Argentina, por medio de la Ley 26.388, reformó la ley sustantiva penal en consonancia con el Convenio de Budapest. En relación con los poderes procesales, este Estado parece enfrentar ciertas dificultades. Aparte del hecho de que Argentina es una federación donde la ley procesal es primordialmente materia de cada provincia, las reglas generales referentes a la evidencia se aplican por analogía a la evidencia electrónica. Este enfoque crea problemas en la práctica. En este país el Congreso está considerando una reforma exhaustiva del Código de Procedimiento Penal. Queda por verse hasta qué punto contendrá las disposiciones específicas necesarias con respecto a la evidencia electrónica.

Colombia enmendó el Código Penal en 2009 mediante la Ley 1273 y el Código de Procedimiento Penal en 2011 mediante la Ley 1453. Por lo anterior la ley sustantiva parece estar en amplia armonía con los estándares internacionales, es decir, con el Convenio de Budapest. Disposiciones de derecho procesal más específicas pueden ser necesarias, incluyendo las enfocadas a la rápida conservación de datos.

Costa Rica había introducido resoluciones específicas referentes al delito cibernético a través de varias enmiendas al Código Penal desde 1999, y más recientemente por medio de la Ley 9048 (noviembre 2012), la Ley 9135 (abril 2013) y la Ley 9177 (noviembre 2013). Adicionalmente, se aplican leyes especiales, por ejemplo, si los delitos involucran los computadores de la administración de impuestos o de la aduana. La Ley penal sustantiva parece estar en gran medida acorde con el Convenio de Budapest. Una ley complementaria sobre el acceso al Convenio ha sido sometida al Parlamento.

En México las enmiendas a las leyes sustantivas y procesales están a punto de concluir, lo cual permitirá a este país completar el acceso al Convenio de Budapest sobre el Delito Cibernético. Se logró amplio consenso entre los principales actores acerca de la necesidad de estas reformas mediante una conferencia en Ciudad de México del 31 de marzo al 2 de abril de 2014. Este evento congregó a los poderes Ejecutivo, Legislativo y Judicial del país, así como a las autoridades en protección de datos, organizaciones de la sociedad civil y la industria. Varios países de América Latina participaron y poco después de terminada la reunión, Paraguay y Perú solicitaron el ingreso al Convenio de

Budapest. Este ejemplo subraya la necesidad de buscar amplio consenso al emprender reformas legislativas.

En Paraguay, la Ley 4439 de 2011 enmendó el Código Penal, el cual ahora incluye la mayoría de las disposiciones del Convenio de Budapest. Se ha establecido un grupo de trabajo para preparar reformas de derecho procesal.

En octubre de 2013, Perú había aprobado la Ley 30096 sobre Delitos Informáticos, encontrando oposición pública respecto a algunas de sus partes, debido a lo cual fue enmendada por la Ley 30171 de abril de 2014. Con esta medida, la ley penal sustantiva se encuentra ahora alineada en gran parte con el Convenio de Budapest. Las herramientas específicas del derecho procesal para manejar la evidencia electrónica no están disponibles todavía y se utilizan otras disposiciones por analogía.

El Convenio de Budapest, por lo tanto, puede servir de lista de verificación para el desarrollo de leyes internas sustantivas y procesales relativas al delito cibernético y la evidencia electrónica.

En muchos países del Caribe se han emprendido también reformas legales o están en curso. Algunos de ellos han usado la Ley Modelo del Commonwealth (2002). Barbados es un ejemplo; la Ley 2005-04 referente al Uso Indebido Informático introdujo un marco legal bastante completo ya en 2005, en relación con el delito cibernético y la evidencia electrónica, incluyendo poderes de derecho procesal. Dado que la Ley Modelo del Commonwealth de 2002 se basaba también en el Convenio de Budapest, el Artículo sobre Uso Indebido Informático de Barbados parece estar en amplia consonancia con los estándares internacionales.

Actualmente en Dominica, varios proyectos de ley están en discusión, entre ellos el proyecto de ley sobre delitos electrónicos. Aparentemente, ahora se le está haciendo frente a las inconsistencias, brechas y amenazas encontradas en un proyecto anterior.

Al parecer, otros países del Caribe están encontrando problemas similares. Una de las razones puede ser la dependencia de "modelos" o "directrices"[7] que no han sido sometidos a prueba.

Conclusiones

La mayoría de los Estados de América Latina y el Caribe están comprometidos con un proceso de reforma legal para enfrentar el desafío que supone el delito cibernético por medio de medidas efectivas de justicia penal.

La OEA a través de REMJA ha recomendado por más de diez años que sus Estados miembros utilicen el Convenio de Budapest sobre el Delito Cibernético como una directriz. El supuesto subyacente es que la legislación basada en este tratado se ha sintonizado lo suficiente con los estándares internacionales como para permitir la efectiva cooperación internacional.

El Convenio de Budapest quedó abierto para su firma en 2001, pero sigue siendo de gran relevancia. El Comité del Convenio sobre el Delito Cibernético (**www.coe.int/tcy**), compuesto por los Estados del Convenio de Budapest –incluyendo ahora la República Dominicana y Panamá– evalúa la implementación del tratado por las Partes, prepara Notas Guía para abordar nuevos fenómenos y puede también preparar instrumentos legales adicionales, tales como protocolos vinculantes. El Convenio y el trabajo del Comité reciben el apoyo de programas de formación de capacidad (**www.coe.int/cybercrime**). Este triángulo de estándares, seguimiento y formación de capacidad crea un proceso dinámico.

Las disposiciones de este tratado son difícilmente controversiales. Por consiguiente, es menos probable que su transposición a la ley interna encuentre oposición si dichas disposiciones se siguen correctamente y con las debidas salvaguardias. Varios países de América Latina y el Caribe han enfrentado resistencia pública importante al tratar de introducir poderes de derecho procesal y delitos más allá de la convención.

Muchos estados latinoamericanos han logrado adoptar disposiciones de derecho penal sustantivo, basándose en gran medida en este tratado. El desafío principal de la región parece ser la adopción de poderes específicos del derecho procesal. Mientras que los códigos de procedimiento penal tienden a ser más bien modernos, la aplicación por analogía de disposiciones que funcionan bien en el mundo físico o la dependencia del principio de libertad probatoria no son suficientes para abordar los desafíos específicos de la evidencia electrónica.

La búsqueda y captura de datos y computadores o la interceptación de comunicaciones para propósitos de justicia penal representan una interferencia con los derechos fundamentales de los individuos. Tal interferencia debe basarse en disposiciones legales específicas. La adopción de poderes de derecho procesal, tales como los previstos por los Artículos 16 a 21 del Convenio de Budapest sujetos a condiciones y salvaguardias ayudarán en el cumplimiento de los requerimientos del Estado de derecho y de los derechos humanos.

En el Caribe, la adopción de poderes de derecho procesal como tal parece representar un inconveniente menor. Los problemas parecen deberse a que los estándares internacionales no siempre se siguen cuando se elaboran las leyes. A veces esto conduce a inconsistencias, brechas, extralimitación y amenazas a los derechos humanos y al Estado de derecho.

Como se indicó al principio, la legislación integral es el fundamento necesario para que la justicia penal dé una respuesta efectiva a los desafíos planteados por el delito cibernético y la evidencia electrónica. Una gran variedad de medidas adicionales para garantizar la aplicación real de las leyes y la cooperación internacional eficiente serán necesarias, incluyendo unidades especializadas en el delito cibernético, de acuerdo también con las recomendaciones del Grupo de Trabajo en Delito Cibernético de las REMJA/OEA[8]. Los fiscales especializados en Argentina (Buenos Aires), Brasil, Chile o Paraguay parecen ser ejemplos de buenas prácticas.

En conclusión, las recomendaciones de las REMJA/OEA respecto de la reforma de la ley penal relativa al delito cibernético y la evidencia electrónica que datan de 2004 hoy en gran medida siguen vigentes. ■

Alexander Seger

Secretario del Comité de la Convención de Delincuencia Cibernética y Jefe de la División de Protección de Datos y Delincuencia Cibernética del Consejo de Europa, Estrasburgo, Francia.

Ha trabajado con el Consejo de Europa (Estrasburgo, Francia) desde 1999. Actualmente es el Jefe de la División de Protección de Datos y Delincuencia Cibernética y el Secretario del Comité de las Partes en la Convención de Budapest sobre Delincuencia Cibernética. Antes de octubre de 2011, Seger dirigió la División de Delitos Económicos, donde se ocupó de los programas de cooperación del Consejo de Europa contra el delito cibernético, la corrupción y el lavado de dinero. De 1989 a 1998 estuvo vinculado con lo que ahora es la Oficina de Naciones Unidas contra la Droga y el Delito en Viena, Austria, en Laos (Jefe de la Oficina) y en Pakistán (Subdirector de la Oficina Regional para Afganistán, Irán y Pakistán) y consultor para la Cooperación Técnica Alemana (GTZ) en materia de control de drogas. Seger es alemán y tiene un doctorado en ciencia política, derecho y antropología social, además de haber realizado estudios en Heidelberg, Burdeos y Bonn.

Notas

1. Secretario Ejecutivo del Comité del Convenio sobre el Delito Cibernético, Consejo de Europa, Estrasburgo, Francia. Las opiniones aquí expresadas no necesariamente reflejan la posición oficial del Consejo de Europa o de los Países Partes del Convenio de Budapest sobre el Delito Cibernético.

2. **http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CM=8&DF=&CL=ENG**

3. **http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/Guidance_Notes/TCY(2013)29rev_GN%20compilation_v3.pdf**

4. Estados que participaron en la negociación del Convenio (Estados miembros del Consejo de Europa, Canadá, Japón, Sur de África y EE.UU.) pueden firmarlo y ratificarlo. Cualquier otro Estado puede convertirse en país firmante mediante el acceso. El resultado es el mismo.

5. **http://www.oas.org/juridico/english/remjaV_recom.pdf**
http://www.oas.org/juridico/english/moj_vi_recom_en.pdf
http://www.oas.org/en/sla/dlc/remja/pdf/recomm_IX.pdf
http://www.oas.org/juridico/english/cyber_experts.htm

6. El Proyecto de Ley 4055 de Guatemala también comprende poderes procesales inspirados en el Convenio de Budapest aunque su adopción sigue pendiente.

7. En diciembre de 2014 el Comité del Convenio sobre Delito Cibernético decidió "señalar los riesgos e inquietudes relacionados con las llamadas "leyes-modelo" sobre delito cibernético preparadas y diseminadas por diferentes organizaciones". **http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/2014/T-CY(2014)22_Plen12AbrRep_V5provisional.pdf**

   Ver también el informe sobre el documento de discusión relacionado: **http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/2014/3021_model_law_study_v15.pdf**

8. **http://www.oas.org/juridico/PDFs/VIIIcyb_recom_en.pdf**

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

CoE | Consejo de Europa

www.coe.int
alexander.seger@coe.int

Economía digital y seguridad en América Latina y el Caribe

WEF | **Foro Económico Mundial**
Consejo sobre la Agenda Global en Seguridad Cibernética

América Latina, el Caribe y el mundo cibernético

En el lapso de unas pocas décadas, Internet, también conocido como el ciberespacio, ha dado un salto de ser una plataforma desconocida, utilizada casi exclusivamente por académicos y conocedores de tecnología, a convertirse en una red de infraestructuras críticas, compitiendo en importancia con la energía o el agua, y presente en casi todos los aspectos de nuestra vida cotidiana. América Latina y el Caribe también han participado en esta transformación cibernética, y aunque la región está lejos de ser líder de la revolución digital, ha logrado avances significativos en los últimos años. En el Networked Readiness Index (NRI) de 2015 del Foro Económico Mundial, un índice que mide la conectividad de las tecnologías de la información y la comunicación (TIC) a través de una serie de factores que van desde la gobernanza, al uso, al impacto económico, 14 de los 23 países de la región incluidos en el estudio aumentaron sus puntajes. Hay muchos ejemplos de gobiernos regionales que han aceptado los retos y oportunidades en el ciberespacio. En 2012, Costa Rica introdujo penas de delincuencia cibernética al código penal de la nación, y se estableció un organismo especializado para responder a las amenazas a la seguridad cibernética (y desde entonces ha subido 9 puntos en la NRI). Perú también aprobó recientemente unas leyes que incluyeron la delincuencia cibernética en el código penal nacional, así como una legislación que establece normas legales de delincuencia cibernética y protección de datos (que le ha significado al Perú subir 16 lugares en el NRI). La infraestructura regional cibernética también se ha mejorado en la región. Bolivia más que duplicó su cobertura de la red móvil entre 2007 y 2015, y le significó un aumento en la clasificación NRI en esta medida, desde el puesto 128 en 2012 a ocupar el primer puesto en 2015. En solicitudes de patentes TIC per cápita del Tratado de Cooperación de Patentes, Barbados pasó de un puesto 34 en 2012, que ya era respetable, a ubicarse en el sexto lugar en 2015, justo por delante de Suiza, Estados Unidos, Holanda y Singapur, todos los pesos pesados de la tecnología. Sin embargo, América Latina y el Caribe deben seguir priorizando el desarrollo del ciberespacio a fin de no quedarse por detrás de otras regiones del mundo en su explotación de oportunidades económicas, así como abordar los desafíos de la seguridad cibernética. Varios factores, incluyendo entornos políticos y reglamentarios, el nivel de habilidad de la fuerza laboral y el desarrollo de sistemas de innovación, ponen a muchos países de América Latina y el Caribe detrás de naciones en niveles similares de desarrollo en el NRI. Brasil, la mayor economía de la región, se ubica en el puesto 84 en disposición en red a la par con la mayoría de otras economías latinoamericanas medianas y grandes; no le va mucho mejor y hasta alcanza posiciones aún más bajas[1]. La clave para permitir el futuro desarrollo en América Latina y el Caribe es entender las tendencias en el ciberespacio y tener soluciones para lograr un impacto potencial en la región.

Margen de mejora

El estado actual de la economía digital en América Latina y el Caribe deja mucho que desear; se caracteriza por un retraso general en calidad, por detrás de otras partes del mundo y con grandes variaciones en la región. De acuerdo con el NRI, el 65% de América Latina y el Caribe se ubica en la mitad más baja de la clasificación, en comparación con el 56% de Asia, el 52% de Oriente Medio y el Norte de África y el 22% de Europa del Este. El mejor clasificado de los países de la región, Chile (puesto 38), está casi 100 puestos por delante del país clasificado como el más bajo, Haití (puesto 137)[2]. Según el Centro de Estudios Estratégicos e Internacionales, América Latina tiene 300 millones de usuarios de Internet, más de la mitad de la población de la región[3]. Esta cifra, sin embargo, oculta grandes disparidades en adopción dentro de la región. Según el Informe Global de Tecnología de Información de 2015, la mayoría de los países de la región se ubican en la mitad inferior del porcentaje de ciudadanos que son usuarios de Internet. Incluso las grandes economías, como

México, Brasil, Argentina, Chile y Colombia, están en la mitad del grupo, ya que solo el 43,5% de los mexicanos son usuarios de Internet y solo el 30,7% de los hogares tienen acceso a Internet. Es aún inferior la participación de gran parte de América Central en el uso de Internet y en tasas de acceso. La disponibilidad de nuevas tecnologías también está rezagada con respecto a muchos otros países que están en el mismo nivel de desarrollo, donde muchas de las grandes economías están en o por debajo de la media, y donde algunos países llegan casi al final de la clasificación. Además, mientras que las tasas de suscripción de telefonía móvil son más altas que las de Estados Unidos, con la excepción de México, Guyana y Haití, la mayor parte de la región se ubica en la mitad más baja en cuanto a las tasas de suscripción de banda ancha móvil de NRI. Sin embargo, y como reflejo de una tendencia de los países de bajos y medianos ingresos que prefieren no tener conexiones de Internet fijas sino más bien contar con Internet móvil, las tasas de suscripción de banda ancha móvil son más altas que las suscripciones fijas, y siguen creciendo. Algunos países ya han adoptado ávidamente la Internet móvil. Costa Rica, por ejemplo, tiene 9,7 suscripciones de banda ancha fija por cada 100 habitantes, mientras que cuenta con

Con todos estos acontecimientos, los riesgos cibernéticos son cada vez más preocupantes y se están convirtiendo en un factor de mayores consideraciones en seguridad y formulación de políticas económicas.

72 suscripciones de banda ancha móvil por cada 100 usuarios.

Con todos estos acontecimientos, los riesgos cibernéticos son cada vez más preocupantes y se están convirtiendo en un factor de mayores consideraciones en seguridad y formulación de políticas económicas. La conciencia de seguridad cibernética ha ido creciendo a medida que se ha reconocido que las amenazas y vulnerabilidades tienen el potencial de frenar la innovación y el avance de la economía basada en Internet, a la vez que ponen en riesgo a los individuos y las organizaciones. Si bien casi todos los países de la región reconocen la necesidad de contar con una estrategia de seguridad cibernética, muy pocos han avanzado más allá de la etapa de tener un esquema. Solo los países más grandes y más ricos de la región cuentan con distintas organizaciones dedicadas a la seguridad cibernética e incluso donde están presentes tales organizaciones, la disposición general cibernética todavía permanece impedida por una falta de coordinación entre los sectores y organismos. El sector privado ha superado al gobierno, en general, en su reconocimiento de la importancia de la seguridad cibernética, mientras que la conciencia entre el público varía en toda la región.

La conciencia seguramente aumentará a medida que más y más servicios gubernamentales se pasen a estar en línea y se generen más conversaciones sobre las implicaciones de la seguridad. Esta conversación ya está en marcha en gran parte de la región en lo que se refiere al comercio electrónico. Las cuestiones de la privacidad en Internet han dado lugar a un mosaico de normas y diferentes niveles de protección en toda la región[4].

Parte del problema con respecto a la escasez de concienciación se deriva de la falta de infraestructura educativa en seguridad cibernética. Pocos países ofrecen programas de educación a nivel posgrado para la seguridad cibernética, y los programas de formación profesional son más comunes, pero varían en calidad. Además, tienen el problema de la difusión de habilidades y la infraestructura de formación. Sin embargo, algo que resaltar es la cuestión legal y reglamentaria en seguridad cibernética. Si bien existe una amplia variación en la cantidad y calidad de legislación cibernética, a la región le va bien en temas sobre los que está interesado el público con respecto a la seguridad en Internet o sea, privacidad, protección de datos y derechos humanos. Las leyes y el procedimiento penal de delincuencia cibernética están bien desarrollados en la región también. Sin embargo, una importante área con margen de mejora es la capacidad de aprovechar las habilidades cibernéticas en la aplicación de la ley, como se indica en los datos proporcionados por los países de América Latina y el Caribe para este estudio.

Estrategias para el éxito cibernético

La diversidad de problemas que enfrentan la seguridad cibernética y la economía digital requieren un conjunto de respuestas innovadoras. El Informe Global de Tecnología de la Información pone de relieve varias políticas gubernamentales sencillas que pueden ayudar a los residentes a aumentar su acceso a Internet. Un enfoque es aumentar el uso gubernamental de las TIC como parte de la política estatal. Esto aumenta la competitividad en el


*****
$$
02/17
175
175

mercado de prestación de servicios, lo que los obliga a innovar mientras simultáneamente socializan la utilidad de Internet entre los que deben utilizarla para interactuar con su gobierno. El informe también recomienda apoyar a las empresas locales de tecnologías de la información, una práctica que no solo fomenta orgánicamente el desarrollo en TIC, sino que también desarrolla una industria que entiende la cultura local mejor, lo que en sí mismo acelera la adopción. En general, los resultados indican que algunos elementos de éxito comunes que respaldan la existencia de un gobierno electrónico eficaz y la mejora de las economías son: el apoyo político por parte de los más altos niveles de autoridad, capital humano bien informado y bien situado (personas que no solo entienden el campo, sino que se pueden conectar con las autoridades adecuadas y comunicar eficazmente sus necesidades) y los recursos financieros (así como la voluntad de dedicar específicamente esos recursos hacia el desarrollo de las TIC)[5].

En un informe de 2015, la Institución Brookings recomendó otras mejores prácticas para mejorar la calidad de la economía digital en formas que pueden implementarse fácilmente en América Latina y el Caribe. Esto incluye soluciones intuitivas como la reducción de costos, mejora de la eficiencia de la red y ampliación de la infraestructura digital. Otras soluciones son más novedosas, como el suministro de contenidos diversos y el fomento del multilingüismo. Brookings incluso sugiere simplemente bajar o eliminar los impuestos sobre los servicios móviles, de acuerdo con un estudio de GSMA[6] que encontró que una disminución del 1% de la carga fiscal conduce a un aumento de la penetración de banda ancha de 1,8%, y un aumento del crecimiento económico del 0,7%, lo que demuestra que incluso medidas relativamente simples que no requieren grandes inversiones en infraestructuras todavía pueden producir resultados[7].

En el frente de la seguridad cibernética, están surgiendo varias tendencias importantes que podrían reducir la vulnerabilidad presente en el sistema y preparar a América Latina y el Caribe para el futuro. Una tendencia en seguridad cibernética hoy es la idea de mejorar la higiene cibernética, o sea, enseñarles técnicas básicas de prevención a las personas y organizaciones para defenderse de ataques cibernéticos de bajo nivel (actualmente la gran mayoría) y permitir que los recursos se concentren en grandes ataques o se desarrollen estrategias de seguridad cibernética nacional. La ventaja de la higiene cibernética es que puede ser concebida de forma barata y difundida ampliamente, y que a menudo puede ser un poco más que una lista de comportamientos o una sesión básica de entrenamiento.

La eficacia de la higiene cibernética puede ser mejorada por otro desarrollo importante: el fomento de la realineación de los incentivos de la industria para promover el pensamiento de primero la seguridad para los vendedores de tecnología. Se trata de guiar a los vendedores hacia la idea de que la seguridad de sus productos es igual de prioritaria a la velocidad o la calidad gráfica. Para poner en marcha este concepto, se están manejando ideas como las siguientes: incentivar a los vendedores con una especie de ganancia adicional al contrato (como un pago al desarrollador de software de una bonificación si pasa un período de tiempo definido sin que haya incidentes de seguridad cibernética); o impulsar la demanda desde el lado del cliente con algún tipo de sello de aprobación, similar a la designación de "sin crueldad" en los alimentos. Una vez más, la inversión pública y la participación en las industrias de TIC locales podrían ser el catalizador que se ocupa de este problema también. Los gobiernos suelen ser algunos de los mayores clientes de algunos proveedores, y sus demandas de contar con productos más seguros podrían forzar cambios en los productos que se van repartiendo y que se venden a consumidores individuales y otras organizaciones.

Los gobiernos suelen ser algunos de los mayores clientes de algunos proveedores, y sus demandas de contar con productos más seguros podrían forzar cambios en los productos que se van repartiendo y que se venden a consumidores individuales y otras organizaciones.

Muchos en la comunidad de seguridad cibernética también abogan por nuevas normas para la colaboración entre las partes interesadas. Estas normas de colaboración no solo les darían a los países, industrias y otros actores reglas de enfrentamiento con el ciberespacio, sino que también serían un marco para mejorar la potencialmente paralizante falta de coordinación entre, y al interior de, las naciones en caso de un evento de seguridad cibernética de gran envergadura. Varios organismos internacionales se están inclinando hacia contar con normas más concretas de colaboración en materia de seguridad cibernética. Esta es un área que está madura para la cooperación regional,

si no mundial, para coordinar mejor las políticas e identificar las mejores prácticas, un proceso que los países de América Latina y el Caribe están bien posicionados para liderar.

En todos estos frentes, la cooperación público-privada es esencial. La participación de las empresas TIC locales, así como la de grandes proveedores internacionales y las organizaciones de la sociedad civil, es la mejor manera de descubrir y compartir las mejores prácticas, y cooperar para diseñar las soluciones más eficaces y eficientes. La naturaleza interdependiente del mundo hiper conectado exige la colaboración. El compromiso del Foro Económico Mundial con los principios de resiliencia cibernética es un ejemplo de un marco que facilita la cooperación entre varios grupos en la seguridad cibernética. Los principios tienen como objetivo reconocer los problemas, desarrollar soluciones prácticas y eficaces, y animar a otros grupos, en particular los clientes y proveedores, para hacer compromisos similares hacia la mejora de la seguridad cibernética. Este tipo de estrategia multisectorial entre múltiples partes interesadas deberá ser aplicada por América Latina y el Caribe, y de hecho todos los demás países, si pretenden construir entornos de seguridad cibernética beneficiosa.

El camino a seguir

Es más fácil decir que se creará una esquina eficiente, próspera y segura dentro del ciberespacio que hacerla, e incluso las naciones mejor preparadas están muy en el límite de sus actualizaciones como para sentirse seguras. Deloitte estima que el acceso mejorado a Internet en el mundo en desarrollo dará lugar a aumentos de la productividad de más del 25%, ganancias de crecimiento del producto interno bruto (PIB) de más del 72%, y sacará a 160 millones de personas de la pobreza[8]. Los beneficios cosechados por una integración más amplia en el ciberespacio no solo tendrán impacto en la billetera, sino en todos los aspectos de la vida, incluyendo la educación, la salud, la inclusión y los derechos humanos[9].

Estas ganancias se basan en la confianza en el ecosistema digital. Ningún país, grande o pequeño, está inmune a los ataques cibernéticos, que provienen de actores estatales y no estatales en un paisaje tecnológico en constante evolución.

El mundo en red está alimentando el crecimiento económico y la mejora de los niveles de vida. También está creando amenazas que eran inimaginables hace apenas una generación. América Latina y el Caribe tienen mucho trabajo por delante. El cerrar las brechas entre países y desarrollar la región será una tarea formidable. Afortunadamente, han demostrado que están a la altura del desafío y ya están utilizando el conocimiento existente para mejorar la capacidad y seguridad cibernéticas. La región se encuentra en una buena posición para aprender no solo de las mejores prácticas, sino para ayudar a crear otras nuevas, y realizar todo su potencial como participante en la economía digital mundial. ■

Notas

1. Dutta, S., Geiger, T., & Lanvin, B. (Eds.). (2015). The Global Information Technology Report (GITR) 2015. Ginebra: World Economic Forum and INSEAD.

2. Fuente: Informe Global sobre Tecnología de la Información del Foro Económico Mundial.

3. Meacham, Carl. "Are Internet Policy and Technology the Keys to Latin America's Future?". Center for Strategic and International Studies. 2 de junio de 2015. **http://csis.org/publication/are-internet-policy-and-technology-keys-latin-americas-future**.

4. Fuente: Informe OEA-BID.

5. Fuente: Informe Global sobre Tecnología de la Información del Foro Económico Mundial.

6. **www.gsma.com**

7. West, Darrell. "Digital Divide: Improving Internet Access in the Developing World through Affordable Services and Diverse Content". Brookings Institution. Febrero 13, 2015. **http://www.brookings.edu/research/papers/2015/02/13-digital-divide-developing-world-west**.

8. Deloitte. "Value of Connectivity: Economic and social benefits of expanding Internet access". Febrero, 2014.

9. Fairchild, Caroline. "For Facebook, Access to Women's Rights Information Is a Basic One". Fortune, agosto de 2014.

WEF | Foro Económico Mundial

www.weforum.org
contact@weforum.org

Desarrollo sostenible y seguro: un marco para las sociedades conectadas resilientes

POTOMAC | **Instituto Potomac**
Melissa Hathaway y Francesca Spidalieri

La penetración de Internet y la adopción más profunda de las tecnologías de la información y la comunicación (TIC) están cambiando muchos aspectos de las economías, los gobiernos y las sociedades del mundo. Todo se ve afectado, desde la forma como se producen, distribuyen y consumen los bienes y servicios, o cómo los gobiernos prestan servicios y difunden información, hasta cómo las empresas y los ciudadanos interactúan y participan en el contrato social. No se pueden ignorar las oportunidades que se asocian a quedar conectados y participando en la economía de Internet y el potencial impacto económico.

Dos tercios de los usuarios de Internet hoy en día viven en el mundo en desarrollo y están impulsando la mayor parte del crecimiento económico mundial. McKinsey estima que en 2011 la contribución global de Internet representó casi el 3% del producto interno bruto (PIB) mundial[1] y el acceso a Internet está creciendo casi cuatro veces más rápidamente en los países en desarrollo que en los desarrollados. Los Estados Miembros de la OEA se han beneficiado de manera importante de la penetración de las TIC y del aumento de la conectividad, que les ha significado abrir nuevas oportunidades económicas y sociales para las poblaciones urbanas y rurales y se han convertido en la plataforma de distribución más grande para la prestación de servicios públicos y privados, incluyendo los servicios bancarios, la educación y la atención en salud a millones de personas desatendidas[2]. Aunque todavía existe una gran disparidad en la penetración de Internet entre los países desarrollados y en vías de desarrollo, la demanda de servicios con acceso a Internet las 24 horas del día, 7 días a la semana (estar siempre encendido), a gran velocidad y capacidad, está aumentando exponencialmente[3].

No es de extrañar, por tanto, que las organizaciones internacionales como la OEA, el Banco Mundial, la Unión Internacional de Telecomunicaciones (UIT) y el Banco Interamericano de Desarrollo (BID), han lanzado y están financiando proyectos para cerrar la brecha de la conectividad y aprovechar los beneficios derivados de la utilización de las TIC para estimular el crecimiento económico, mejorar la prestación y la capacidad de servicios, impulsar las ganancias de la productividad y la innovación y para promover el buen gobierno. Muchos de sus informes y publicaciones alaban el papel que desempeñan las TIC en la promoción de estrategias de desarrollo de estos países y en la responsabilidad de gobierno y proporcionan indicadores fuertes para apoyar una mayor conectividad a Internet y ecosistemas digitales más extensos. El Banco Mundial, por ejemplo, estima que cuando el 10% de la población en países en desarrollo está conectado a Internet, el PIB del país crece en un 1% a un 2%[4], mientras que el Foro Económico Mundial informó que incluso duplicar el uso de datos de banda ancha móvil puede conducir a un aumento del 0,5% del crecimiento del PIB[5]. Al mismo tiempo, sin embargo, el poder transformador de las TIC como un catalizador para el crecimiento del PIB y el desarrollo social puede ser socavado fácilmente si los riesgos de seguridad asociados con la proliferación de infraestructura de las TIC y de aplicaciones de Internet no se equilibran adecuadamente con un plan integral de seguridad cibernética y resiliencia[6].

Hay dos intereses enfrentados en la realización de la promesa y el potencial de las TIC y de Internet. En primer lugar, hay una agenda digital y una visión económica que promete generar ingresos y empleo, proporcionar acceso a los negocios y la información, aumentar la productividad y la eficiencia, permitir el aprendizaje electrónico, mejorar las habilidades de la fuerza laboral, facilitar las actividades del gobierno y extender la prosperidad mediante el crecimiento del PIB y así reducir la pobreza. Sin embargo, la única manera en que los países pueden lograr tales resultados es si su programa de desarrollo de las TIC es sostenible.

- Ambientalmente, mediante la mitigación de los impactos ambientales negativos (por ejemplo, emisiones de gases de efecto invernadero, generación de basura electrónica, degradación del medio ambiente, etc.) del mayor crecimiento de las redes y los dispositivos de las TIC.

- En lo económico, al proporcionar un acceso a Internet más asequible, fiable y persistente para todos[7].

- En lo social, mediante la maximización de la contribución potencial de las TIC a la equidad social y la inclusión.

- En lo político, al permitir la participación ciudadana en los procesos del gobierno y la toma de decisiones.

En segundo lugar, se encuentra la seguridad. No es suficiente que el aumento de la conectividad a Internet sea sostenible: también es necesario que dicha conectividad sea segura y resistente. De hecho, nuestra dependencia de esta compleja infraestructura ha venido con un precio: al conectar tantos aspectos de nuestra economía y servicios vitales a Internet, también nos hemos expuesto a una serie de actividades cibernéticas nefastas que pueden socavar la disponibilidad, integridad y resiliencia de esta infraestructura central, lo que ha amenazado los beneficios económicos y también tecnológicos, políticos y sociales de Internet. Por ejemplo, varios de los países del Grupo de los 20 (G-20) han estimado que están perdiendo al menos el 1% de su PIB debido al delito cibernético, el robo de propiedad intelectual y otras actividades electrónicas fraudulentas. Ninguna nación puede darse el lujo de perder ni un 1% de su PIB por cuenta de actividades ilícitas cibernéticas. A medida que las tecnologías informáticas y de comunicaciones se arraigan más en la economía global y a medida que entramos en la era de la "Internet de las cosas" (IoT, por sus siglas en inglés), seguirán aumentando los incentivos para poner en peligro la seguridad de estos sistemas. Debemos enfrentar que las amenazas a nuestra sociedad conectada están superando nuestras defensas y el crecimiento del PIB se está erosionando cada día. En pocas palabras, la inseguridad cibernética es un impuesto al crecimiento y los países deben demostrar un compromiso con la seguridad y la resiliencia para preservar la promesa de conexión y realizar todo el potencial de la economía de Internet.

Este entrelazamiento entre infraestructura e Internet es una vulnerabilidad estratégica para todas las sociedades conectadas[8] y hay mucho en juego. El impacto positivo de Internet en los países, comunidades, empresas y ciudadanos por igual solo puede sostenerse si el servicio es accesible, disponible, asequible, seguro, interoperable, resiliente y estable[9]. Esta es la razón por la cual Internet y su propuesta subyacente de valor se han convertido en un imperativo de seguridad tanto económico como nacional. Los líderes mundiales deben lidiar con el hecho de que su infraestructura de Internet y servicios orientados al ciudadano son vulnerables a la interferencia y que su dependencia económica de Internet no les permitirá abandonar el camino de adopción en el que se encuentran[10].

La OEA y el BID han centrado muchos de sus esfuerzos en la creación y generación de una cultura de seguridad cibernética en la región y se han comprometido a trabajar con sus Estados Miembros para luchar contra la delincuencia cibernética, fortalecer la resiliencia cibernética y promover estrategias sostenibles de desarrollo de las TIC. En particular, la OEA y el BID están ayudando a los países de América Latina y el Caribe a anticipar y reaccionar ante las nuevas amenazas cibernéticas.

Desafortunadamente, a la mayoría de las naciones aún les falta hacer eso. La mayoría de las estrategias de desarrollo defienden los beneficios de la comunicación de banda ancha rápida, asequible y de largo alcance y mayor dependencia de los servicios orientados a Internet en términos de crecimiento económico. Pero pocas toman en cuenta igualmente la exposición y los costos de servicios críticos menos resilientes, interrupción del (de los) servicio(s), el delito electrónico, el robo de identidad, robo de propiedad intelectual, fraude y otras actividades de explotación de la hiper-conectividad de las TIC en términos de pérdidas económicas. Los líderes mundiales deben reconocer que el aumento de conectividad a Internet puede llevar a un crecimiento económico, pero solo si esa conexión a Internet, y la infraestructura de las TIC que la soporta, es segura. Si los países no invierten por igual en la seguridad de su infraestructura básica y la resiliencia de sus sistemas, los costos impuestos por las actividades cibernéticas nefastas gravarán su crecimiento económico[11].

Los líderes mundiales pueden aprovechar el poder económico de las TIC y al mismo tiempo evitar daños irreversibles a largo plazo a la economía, salud, seguridad y la resiliencia de sus países solo si la seguridad juega un papel igualmente importante en sus estrategias de desarrollo. Después pueden aprovechar las políticas, leyes, reglamentos, normas, incentivos de mercado y otras iniciativas para proteger el valor de sus inversiones digitales y preservar la seguridad de su conectividad. Pueden perseguir y financiar iniciativas de seguridad cibernética que disminuyen los riesgos y aumentan la resiliencia.

El Cyber Readiness Index (CRI), desarrollado por el Instituto Potomac, se ocupa de estas cuestiones y proporciona el modelo a seguir para los países[12]. Ayuda a que un país pueda comprender su enredo entre Internet e infraestructura y su consecuente vulnerabilidad. También proporciona una base sólida sobre la cual cada país puede evaluar su madurez en seguridad cibernética. Identifica siete elementos esenciales donde se puede utilizar la seguridad cibernética para proteger el valor y la integridad de las inversiones anteriores en TIC y activar la economía de Internet, a saber: la estrategia nacional y la formulación de políticas; la capacidad de respuesta a incidentes; iniciativas de

delito electrónico y las necesidades de capacidad de las fuerzas del orden; iniciativas de compartir información; la inversión en investigación y desarrollo (I+D); la diplomacia y el comercio; y la capacidad militar y las iniciativas de defensa cibernética.

Adoptar un marco de seguridad y conocer el nivel de preparación cibernética de un país es ciertamente esencial. El primer paso que debe tomar un país para desarrollar este marco es articular una estrategia nacional de seguridad cibernética válida. Esta estrategia debe: describir el problema en términos económicos; identificar la autoridad competente que garantice la correcta ejecución de la estrategia; incluir objetivos específicos, medibles, alcanzables, basados en el tiempo y en los resultados del plan de implementación; y reconocer la necesidad de comprometer recursos limitados (por ejemplo, voluntad política, dinero, tiempo y personas) en un entorno competitivo para lograr los resultados económicos necesarios. Varios Estados Miembros de la OEA han comenzado a diseñar este tipo de estrategias para gestionar la seguridad cibernética y han dado pasos importantes en el desarrollo de políticas relacionadas con cibernética, doctrinas, marcos jurídicos y la capacidad técnica. Colombia, en particular, ha tenido una política nacional para la seguridad cibernética y defensa cibernética operando durante varios años (CONPES 3701)[13] y recientemente ha estado trabajando en una nueva estrategia integral de Seguridad Cibernética Nacional para reflejar su compromiso de estar cibernéticamente lista en las áreas de gobernanza enfocada y liderazgo institucional a nivel nacional, con el fortalecimiento de la capacidad de respuesta a incidentes y las asociaciones público-privadas y el desarrollo de la conciencia cibernética y la profundización de la educación cibernética.

Otros elementos esenciales son la posibilidad de los países de establecer y mantener tanto una capacidad nacional de respuesta a incidentes como un mecanismo de intercambio de información que permita el intercambio de inteligencia procesable entre el gobierno y la industria. La mayoría de los países de América Latina y el Caribe ya han establecido y puesto en funcionamiento los Equipos de Respuesta ante Emergencias Informáticas (CSIRT, por sus siglas en inglés) o capacidades y están ampliando los servicios prestados por estas unidades más allá de tener funciones reactivas, e incluyen servicios proactivos, preventivos, educativos y de gestión de la seguridad. El establecimiento de mecanismos de intercambio de información formal, por otro lado, sigue siendo un reto importante en la región, aunque la mayoría de las autoridades nacionales mantienen líneas abiertas y activas de comunicación y colaboración con sectores críticos y empresas clave.

El tener una estrategia y compromiso es solo el comienzo. Otros aspectos clave para estar listos cibernéticamente incluyen el compromiso de un país de proteger a la sociedad contra el delito cibernético a través de mecanismos legales y regulatorios nacionales e internacionales y la capacidad para luchar contra el crimen cibernético, incluyendo la capacitación de las fuerzas del orden, especialistas forenses, juristas y legisladores. Panamá, por ejemplo, es miembro de la Convención de Budapest sobre el delito cibernético y ha trabajado incansablemente para actualizar la legislación nacional para combatir más eficazmente la delincuencia cibernética y fortalecer la protección de datos. Además, ha establecido una Fiscalía Especial de Delitos contra la Propiedad Intelectual y Seguridad de la Información, que forma parte del Ministerio Público y una Unidad de Investigación de Delitos Cibernéticos, dependiente de la Dirección de Investigación Judicial, para servir como las agencias líderes para la investigación y el enjuiciamiento de los delitos cibernéticos.

Los países también deben invertir en investigación básica y aplicada de seguridad cibernética (innovación) y financiar generosamente las iniciativas de seguridad cibernética si quieren aprovechar las oportunidades que ofrece la economía de Internet, mientras que mantienen una fuerte postura de seguridad cibernética. Chile, por ejemplo, ha aprovechado al máximo su alta conectividad y ha puesto en marcha varias iniciativas para desarrollar su industria de alta tecnología. El programa Start-Up Chile, a cargo de la Agencia de Desarrollo Económico de Chile (CORFO) a través de InnovaChile, está ayudando a transformar a dicho país en un centro de innovación y de espíritu empresarial en América Latina. Este programa acelerador busca atraer empresarios de fase inicial y alto potencial, para arrancar sus nuevas empresas en Chile, usándolo como una plataforma para luego lanzarse globalmente. Además, la Universidad de Chile ofrece títulos avanzados en seguridad cibernética y se espera que la comunidad empresaria proporcione conferencias y tutorías adicionales.

Otro elemento clave a menudo pasado por alto es la voluntad y la capacidad de los países de participar diplomáticamente o durante las negociaciones comerciales sobre cuestiones relacionadas con la cibernética. Guatemala, por ejemplo, mostró una fuerte capacidad diplomática cibernética en 2012 al presidir el Comité Interamericano contra el Terrorismo de la OEA. El país lideró una Declaración sobre el Fortalecimiento de la Seguridad Cibernética en las Américas, que dio lugar a su adopción unánime y elevó el reconocimiento de la seguridad y la resiliencia de la infraestructura de información crítica, especialmente para las instituciones esenciales para los sectores de seguridad nacional, como comunicaciones, energía, finanzas y transporte[14].

Por último, los Estados están empezando a aprovechar la capacidad de sus fuerzas armadas nacionales y/o agencias de defensa relacionadas para defender a su país cinéticamente y proporcionar una defensa similar a través del ciberespacio, en respuesta a las amenazas de seguridad cibernética. Brasil, por ejemplo, ya ha desarrollado capacidades avanzadas de defensa cibernética y, recientemente, estableció un Comando de Defesa Cibernética y una Escuela de Defensa Cibernética Nacional, que contará con representantes de las tres fuerzas armadas brasileñas.

Mientras que la penetración de Internet y la modernización de la infraestructura se están expandiendo y están madurando rápidamente, es esencial que los países establezcan inicialmente un marco para las sociedades resilientes conectadas, incluyendo en este la preservación de la promesa del dividendo TIC que es desarrollo sostenible con seguridad. A medida que las poblaciones de la región continúan avanzando, creciendo y expandiendo sus oportunidades económicas y sociales y los países comienzan a adoptar el Internet de las cosas, se vuelve cada vez más importante abordar el riesgo cibernético, seguridad, resiliencia y exposición en conjunto con los objetivos y el desarrollo sostenibles. Los países deben indicar que la seguridad, la sostenibilidad y la resiliencia son igualmente importantes para su programa de crecimiento. Iniciativas de la OEA y el BID están acelerando la capacidad de las naciones de América Latina y Caribe de poner en funcionamiento las políticas, planes, leyes y regulaciones para promover el desarrollo y el uso de las TIC[15] y están volviendo prioritaria la seguridad cibernética en su agenda social y de política. ■

Melissa Hathaway

Experta en la política de ciberespacio y seguridad cibernética. Es Asesora Senior en el Centro Belfer para Ciencia y Asuntos Internacionales de la Escuela Kennedy de Harvard y se desempeña como Asociada Senior y miembro de la Junta de Regentes del Instituto Potomac de Estudios Políticos. Trabajó en dos administraciones presidenciales, durante las cuales encabezó la Revisión de las Políticas de Ciberespacio para el presidente Obama y lideró la Iniciativa de Seguridad Cibernética Nacional Integral para el presidente George W. Bush. Ha desarrollado una metodología única para evaluar y medir el nivel de preparación ante ciertos riesgos de seguridad cibernética, conocida como el Índice de Preparación Cibernética y está aplicando su metodología en 125 países.

Francesca Spidalieri

Es investigadora principal para el Liderazgo Cibernético en el Centro Pell, en Salve Regina University, y está vinculada como experta en la materia para el Proyecto Índice de Preparación Cibernética del Instituto Potomac de Estudios Políticos. Su investigación académica y publicaciones se han centrado en el desarrollo de liderazgo cibernético, la gestión de riesgos cibernéticos, educación y conciencia cibernética y el desarrollo de la fuerza laboral de seguridad cibernética.

Notas

1. McKinsey Global Institute. "Internet Matters: The Net's Sweeping Impact on Growth, Jobs, and Prosperity". Mayo 2011. p. 12. **https://www.nwoinnovation.ca/upload/documents/mgi-Internet-matters-report.pdf**.

2. The Global Connectivity Group for Sustainable Development. "ICTs, The Internet and Sustainability". Febrero 27, 2013. **https://ictstheInternetandsustainability.wordpress.com**.

3. Banco Mundial. "Information and Communications for Development 2009: Extending Reach and Increasing Impact". p. 127.

4. Banco Mundial. "Overview". Information & Communication Technologies Program. **http://www.worldbank.org/en/topic/ict/overview**.

5. Foro Económico Mundial. "The Global Information Technology Report 2015". Abril 2015. p. 32.

6. European Union Institute for Security Studies. "Riding the Digital Wave: The Impact of Cyber Capacity Building on Human Development". Report nº 21. Diciembre 2014. p. 54.

7. Unión Internacional de Telecomunicaciones. "Connect 2020 Agenda for Global Telecommunication/ICT development". 2014. **http://www.itu.int/en/connect2020/Pages/default.aspx**.

8. Melissa Hathaway. "The Role of the State in Cyber Defense". 4th Conference on Information Security and Cyber Defense. Budapest, Hungría, 8 de septiembre de 2014.

9. Melissa Hathaway. "Connected Choices: How the Internet Is Challenging Sovereign Decisions". American Foreign Policy Interests 36, nº 5. Noviembre 2014. p. 301.

10. Ibid.

11. Melissa Hathaway. "Cyber Readiness Index 2.0 & Lessons Learned in the Design of National Cyber Security Strategies". OAS-IDB Regional Workshop on Cyber Security Policies. Washington D.C., Octubre 23, 2014.

12. Melissa Hathaway et al.. "Cyber Readiness Index 2.0". Potomac Institute for Policy Studies. Borrador presentado en febrero de 2015 para ser publicado en septiembre de 2015.

13. CONPES 3701 definió los principios rectores de la seguridad cibernética; definió las funciones y responsabilidades; resaltó las áreas prioritarias para la acción y la inversión por parte de las autoridades gubernamentales; y entregó el mandato para ColCERT, el organismo nacional responsable de la respuesta a incidentes cibernéticos y la coordinación entre las partes interesadas a nivel nacional.

14. Comité Interamericano contra el Terrorismo. Declaración "Fortalecimiento de la Seguridad Cibernética en las Américas". 7 de marzo de 2012. **https://www.sites.oas.org/cyber/Documents/Declaracion%20del%20Fortalecimiento%20de%20la%20Seguridad%20en%20las%20Americas.pdf**

15. Organización de los Estados Americanos. Declaración de Asunción para el Cuadragésimo Período Ordinario de Sesiones de la Asamblea General de la OEA: "Desarrollo con Inclusión Social". **http://www.oas.org/es/centro_noticias/comunicado_prensa.asp?sCodigo=D-005/14**

16.

POTOMAC INSTITUTE FOR POLICY STUDIES

POTOMAC | Instituto Potomac

www.potomacinstitute.org
contact@potomac.org

Marco metodológico

Sinopsis

Profesora Sadie Creese, Centro Global de Capacidad sobre Seguridad Cibernética
Universidad de Oxford

La manera en que los Estados-nación y las regiones abordan la capacidad de seguridad cibernética es esencial para contar con una seguridad cibernética eficaz, eficiente y sostenible. Es imperativo que como comunidad internacional aboguemos por tener un enfoque integral y holístico para la construcción de capacidad de seguridad cibernética para fomentar una economía digital segura y competitiva, y para obtener los beneficios que la participación en el ciberespacio puede aportarles a las sociedades y las personas en todas partes. La OEA y el BID han incorporado este enfoque de desarrollo de capacidades al núcleo de nuestra cooperación como miembros de esta comunidad internacional.

Para que las personas puedan comprender mejor cómo será una seguridad cibernética eficaz a través de la experiencia y el aprendizaje del mundo, el Centro, por medio de una amplia consulta a 200 expertos internacionales del gobierno, la academia, la industria y la comunidad técnica, ha desarrollado un modelo para entender la madurez de las capacidades de seguridad cibernética. El Modelo de Madurez de Capacidad de Seguridad Cibernética (CMM, por sus siglas en inglés) toma en cuenta las consideraciones de seguridad cibernética a través de cinco diferentes áreas/dimensiones de la capacidad, entendiendo que cada dimensión no es necesariamente independiente de las otras.

Las cinco dimensiones son: Políticas y estrategia nacional de seguridad cibernética; Cultura cibernética y sociedad; Educación, formación y competencias en seguridad cibernética; Marco jurídico y reglamentario; y Normas, organización y tecnologías. Cada dimensión ofrece una serie de factores e indicadores de capacidad cibernética para que una nación comprenda la etapa de madurez en cada consideración específica. Se han identificado cinco etapas de madurez y estas varían desde una etapa inicial, en la cual una nación puede que haya apenas comenzado a considerar la seguridad cibernética, hasta un escenario dinámico, en el cual una nación es capaz de adaptarse rápidamente a los cambios en el panorama de la seguridad cibernética en relación a las amenazas, las vulnerabilidades, los riesgos, la estrategia económica o el cambio de las necesidades internacionales.

El CMM es el primero de su tipo en términos de extensión y profundidad en cada aspecto de capacidad de la seguridad cibernética. Está construido sobre una base de consulta de múltiples partes interesadas y el respeto de los derechos humanos, equilibrando cuidadosamente la necesidad que se tiene de seguridad para permitir el crecimiento económico y la sostenibilidad, al tiempo que se respetan el derecho a la libertad de expresión y el derecho a la privacidad.

Con el fin de asegurar que el CMM se pueda aplicar a las características específicas regionales de América Latina y el Caribe, el Banco Interamericano de Desarrollo, la Organización de Estados Americanos y Oxford desarrollaron una herramienta de aplicación para la región. Esta herramienta de aplicación, que utiliza el CMM como su base, está diseñada para ayudar a una nación a evaluar su capacidad de seguridad cibernética actual y disponer dónde invertir para permitir que haya una capacidad más madura y resiliente, y mejorar la seguridad de la infraestructura nacional. La herramienta de aplicación, por lo tanto, sirve para ayudarles a los gobiernos o naciones a hacer inversiones estratégicas mejor informadas en capacidad de seguridad cibernética de acuerdo con las prioridades nacionales contrapuestas.

Hay un puñado de países de todo el mundo que puede estar en una etapa superior de madurez. Es poco probable que una nación evidencie estar en una etapa de madurez dinámica por todos los factores y los indicadores de las cinco dimensiones descritas en la herramienta de aplicación y CMM. Ha habido grandes avances en capacidad cibernética en América Latina y el Caribe en la mejora de la conectividad en la región. Con el aumento de las tasas de penetración de Internet, no es de extrañar que el gobierno y los interesados de la industria estén preocupados por la falta de capacidad de la seguridad cibernética y algunos hayan

comenzado el proceso de considerar la seguridad cibernética una prioridad nacional.

Es muy alentador ver que recientemente algunas naciones han dado el importante paso de formar y publicar una estrategia nacional de seguridad cibernética, proyectando las prioridades para las inversiones en estos países, con énfasis en el aseguramiento de la infraestructura crítica nacional, el desarrollo de la legislación para luchar eficazmente contra el delito cibernético y el establecimiento de marcos para la divulgación responsable de los incidentes.

El Modelo de Madurez de Capacidad de Seguridad Cibernética (CMM) toma en cuenta las consideraciones de seguridad cibernética a través de cinco diferentes áreas/dimensiones de la capacidad, entendiendo que cada dimensión no es necesariamente independiente de las otras.

Los datos recogidos en este estudio mostraron que varios países poseen un CSIRT nacional o están en el proceso de establecer formalmente una capacidad de respuesta a incidentes. En los lugares donde aún no se han desarrollado estrategias nacionales de seguridad cibernética, se observa una tendencia emergente en la que un CSIRT nacional adquiere un papel más amplio en la coordinación de la seguridad cibernética y cooperación con la policía en los casos de ataque.

Hay un gran valor en el desarrollo de una estrategia nacional de seguridad cibernética a través de consultas de múltiples partes interesadas y enfoques interministeriales. Hay excelentes ejemplos de comités directivos interministeriales y/o grupos de trabajo de la región, que incluyen representación de la sociedad civil y la industria. Por ejemplo, como indica el informe, Jamaica lanzó su Estrategia Nacional de Seguridad Cibernética en enero de este año. Al hacerlo, el país creó el Grupo de Trabajo Nacional de Seguridad Cibernética. El ejercicio de desarrollar una estrategia nacional es valioso en muchos aspectos, ya que congrega en una mesa a todas las partes interesadas que pueden tener la responsabilidad de la seguridad cibernética. Este esboza las prioridades nacionales, mandatos y autoridades relativas, teniendo en cuenta las prioridades nacionales elaboradas para una nación o región. El Centro de Capacidad tuvo el privilegio, mediante la cooperación con la OEA, de contribuir al desarrollo de la Estrategia Nacional de Seguridad Cibernética de Jamaica, y vio su lanzamiento en enero de este año.

También se resalta la cooperación con organizaciones internacionales como INTERPOL en el combate efectivo de la delincuencia cibernética, potenciando las capacidades para combatir la delincuencia mediante el desarrollo de marcos legislativos, pero también la formación investigadora especialista, el tratamiento de pruebas electrónicas y la formación de jueces y la fiscalía. También es muy alentador ver acuerdos intra-regionales, como la Convención Interamericana sobre Asistencia Mutua en Materia Penal, la cual ha sido destacada por muchos países miembros como un mecanismo importante en la lucha contra los delitos informáticos. Otro hecho alentador es la cooperación regional con ejemplos de Suriname abogando en nombre de la región en los foros internacionales.

La promoción de las competencias de seguridad cibernética a través de la construcción de una base de conocimientos y la sensibilización en materia de seguridad cibernética es una prioridad que se evidencia en la región. Los esfuerzos de sensibilización son una herramienta vital para el cambio de comportamiento en seguridad cibernética, pero deben aplicarse en conjunto con otras estrategias que puedan influenciar. Chile en los últimos años ha comenzado la realización de campañas de sensibilización dirigidas como la campaña de Internet Segura y la campaña de Consumidor Digital, que pretenden aumentar la conciencia de seguridad cibernética en grupos demográficos particulares. Es muy importante introducir comportamientos positivos hacia la seguridad de la información, que pueden resultar en una práctica segura habitual. Estas prácticas, con el apoyo de tecnologías de seguridad fáciles de utilizar, proporcionan una base sólida para una sociedad cibernética resiliente.

También son dignos de mención los incentivos para la formación y la educación en la región. Hay ofertas destinadas a educación y formación en seguridad de la información. Se ofrecen cursos sobre seguridad cibernética en las universidades, los cuales otorgan títulos de grado y maestría. Si bien este informe no detalla los cursos que se ofrecen, sí indica que algunas universidades de la región de América Latina y el Caribe están solicitando acreditación en los cursos de seguridad cibernética, por ejemplo en Bolivia, Brasil, Colombia, Panamá, Perú, entre otros.

América Latina y el Caribe es digna de elogio en este estudio sin precedentes, donde se hace el mapeo de la capacidad de la seguridad cibernética en la región. A través del impulso del BID y la OEA, ALC es la primera en el mundo en realizar esta profunda y amplia comprensión de la capacidad de la seguridad cibernética en una región entera utilizando el modelo CMM. Además de promover un enfoque integral para el desarrollo de capacidades de seguridad cibernética a nivel nacional, este informe de América Latina y el Caribe significa que los gobiernos miembros, junto con el apoyo de la comunidad donante e internacional, pueden hacer inversiones más estratégicas de colaboración en la capacidad de la seguridad cibernética, capitalizando el recurso existente y dirigiendo mejor la inversión extranjera.

A través del impulso del BID y la OEA, ALC es la primera en el mundo en realizar esta profunda y amplia comprensión de la capacidad de la seguridad cibernética en una región entera utilizando el modelo CMM.

Las etapas de madurez descritas en el modelo no están diseñadas para ser ni estáticas ni solo progresivas. Se entiende que una nación puede decidir, por ejemplo, invertir fuertemente en la mejora de sus marcos legislativos y capacidad de justicia penal, lo que puede hacer avanzar su madurez en un área de la capacidad desde una etapa inicial hasta una ya establecida. Por otro lado, si una nación deja de llevar a cabo una campaña de sensibilización, ya no mantendrá su etapa de madurez alta y volverá a una etapa anterior. Este ejercicio se ha empeñado en capturar el estado actual de la capacidad de la seguridad cibernética y, con el apoyo continuo de excelentes socios como la OEA y el BID, el CMM se podrá aplicar de nuevo para dar cuenta de los aumentos de la capacidad cibernética en América Latina y el Caribe. ■

El **Centro Global de Capacidad sobre Seguridad Cibernética de la Universidad de Oxford** fue establecido en 2013, para construir una comprensión global de prácticas eficientes y eficaces de creación de capacidad de seguridad cibernética mediante la investigación académica rigurosa. El trabajo del Centro está dirigido por los líderes de opinión del mundo en este campo. En 2014, el Centro de Capacidad, en cooperación con el BID y la OEA, diseñó una herramienta de aplicación para que la región implementara el CMM para poner en evidencia este estudio.

Sadie Creese

Profesora de ciberseguridad en el Departamento de Ciencias de la Computación en la Universidad de Oxford, es miembro del Consejo de Administración del Worcester College de Oxford. Asimismo, funge como Directora del Centro Global de Capacidad sobre Seguridad Cibernética en el Martin School de Oxford y miembro del Comité de Coordinación para CyberSecurity@Oxford. Creese lidera y gestiona grandes programas de investigación interdisciplinarios, supervisa proyectos de grado, y enseña a nivel de postgrado para el Centro de Formación Doctoral en Seguridad Cibernética y Riesgo Cibernético para el MBA y programas ejecutivos en la Saïd Business School. Además, se dedica a un amplio portafolio de investigación en seguridad cibernética que abarca modelos de capacidad de seguridad cibernética, modelado del daño cibernético, conocimiento de la situación, analítica visual, propagación y comunicación del riesgo, modelado y detección de amenazas, defensa de la red, fiabilidad y resiliencia, confianza y privacidad. Desde 2003, ha participado en trabajos de investigación con otros profesionales, como psicólogos, sociólogos, economistas, politólogos, abogados, criminólogos y filósofos, entre otros. Creese tiene experiencia en filosofía, matemáticas y ciencias de la computación y ha trabajado profesionalmente en organizaciones comerciales, gubernamentales y académicas. Antes de incorporarse a Oxford en octubre de 2011, fue Profesora y Directora de Seguridad Electrónica del Laboratorio Digital Internacional de la Universidad de Warwick. Creese se vinculó a Warwick en 2007 después de haber trabajado con QinetiQ. En Warwick, su puesto más reciente fue como Directora de Programas Estratégicos para la División de Gestión de Confianza de la Información. Sus publicaciones recientes incluyen trabajos sobre temas de detección de amenazas internas, analítica visual de ataque cibernético, predicción de la propagación del riesgo cibernético, atribución de identidad en espacios físicos y cibernéticos, privacidad personal de cara a datos grandes, vulnerabilidad de las identidades en contextos de redes sociales, métricas de confiabilidad de los datos de origen abierto y la mejor manera de comunicar el riesgo cibernético.

Universidad de Oxford
https://www.cybersecurity.ox.ac.uk
enquiries@cybersecurity.ox.ac.uk

Capacidad de seguridad cibernética

Los datos utilizados para este informe se recogieron a través de una encuesta en línea desarrollada en colaboración con el Centro Global de Capacidad sobre Seguridad Cibernética (GCSCC) sobre la base del Modelo de Madurez de Capacidad de Seguridad Cibernética (CMM, por sus siglas en inglés) desarrollado por el GCSCC. La encuesta en línea fue traducida en dos idiomas (inglés y español) y se puso a prueba inicialmente con visitas a cuatro países piloto (Colombia, Costa Rica, Jamaica y Saint Kitts y Nevis), para luego ser administrada a un amplio sector de partes interesadas nacionales.

La encuesta en línea fue distribuida a los Estados Miembros con una contraseña segura y se pidió a los puntos de contacto de cada Estado Miembro distribuirla a las partes interesadas nacionales que tendrían la información necesaria para proporcionar el panorama más completo de la seguridad cibernética en sus respectivos países. Se recibieron más de 260 respuestas y la información fue luego agregada y revisada teniendo en cuenta fuentes de información complementarias.

Los datos fueron analizados utilizando los 49 indicadores del CMM, que se dividen entre cinco dimensiones: 1) Políticas y estrategia nacional de seguridad cibernética ("Políticas y estrategia"); 2) Cultura cibernética y sociedad ("Cultura y sociedad"); 3) Educación, formación y competencias en seguridad cibernética ("Educación"); 4) Marco jurídico y reglamentario ("Marco jurídico"); y 5) Normas, organizaciones y tecnologías ("Tecnologías"). Cada dimensión tiene múltiples factores que contribuyen a un estado más maduro de capacidad en materia de seguridad cibernética. Cada factor tiene varios niveles de indicadores que describen un estado de madurez. Los diferentes niveles de madurez ayudan al encuestado a seleccionar el nivel que es más aplicable a su experiencia de la seguridad cibernética en el país.

Los resultados del análisis fueron enviados a cada Estado Miembro para su validación. Perfiles de país se desarrollaron a continuación para cada Estado Miembro, teniendo en cuenta datos estadísticos sobre la población del país, la penetración de Internet y los abonos a teléfonos celulares (todas las estadísticas provenientes de Banco Mundial banco de datos, última acceder noviembre, 2015 en http://databank.bancomundial.org/data/home.aspx).

Política y estrategia

Estrategia nacional de seguridad cibernética oficial o documentada
Desarrollo de la estrategia
Organización
Contenido

Defensa cibernética
Estrategia
Organización
Coordinación

Cultura y sociedad

Mentalidad de seguridad cibernética
En el gobierno
En el sector privado
En la sociedad

Conciencia de seguridad cibernética
Sensibilización

Confianza en el uso de Internet
En los servicios en línea
En el gobierno electrónico
En el comercio electrónico

Privacidad en línea
Normas de privacidad
Privacidad del empleado

Educación

Disponibilidad nacional de la educación y formación cibernéticas
Educación
Formación

Desarrollo nacional de la educación de seguridad cibernética
Desarrollo nacional de la educación de seguridad cibernética

Formación e iniciativas educativas públicas y privadas
Capacitación de empleados en seguridad cibernética

Gobernanza corporativa, conocimiento y normas
Comprensión de la seguridad cibernética por parte de empresas privadas y estatales

Marcos legales

Marcos jurídicos de seguridad cibernética
Para la seguridad de las TIC
Privacidad, protección de datos y otros derechos humanos
Derecho sustantivo de delincuencia cibernética
Derecho procesal de delincuencia cibernética

Investigación jurídica
Cumplimiento de la ley
Fiscalía
Tribunales

Divulgación responsable de la información
Divulgación responsable de la información

Tecnologías

Adhesión a las normas
Aplicación de las normas y prácticas mínimas aceptables
Adquisiciones
Desarrollo de software

Organizaciones de coordinación de seguridad cibernética
Centro de mando y control
Capacidad de respuesta a incidentes

Respuesta a incidentes
Identificación y designación
Organización
Coordinación

Resiliencia de la infraestructura nacional
Infraestructura tecnológica
Resiliencia nacional

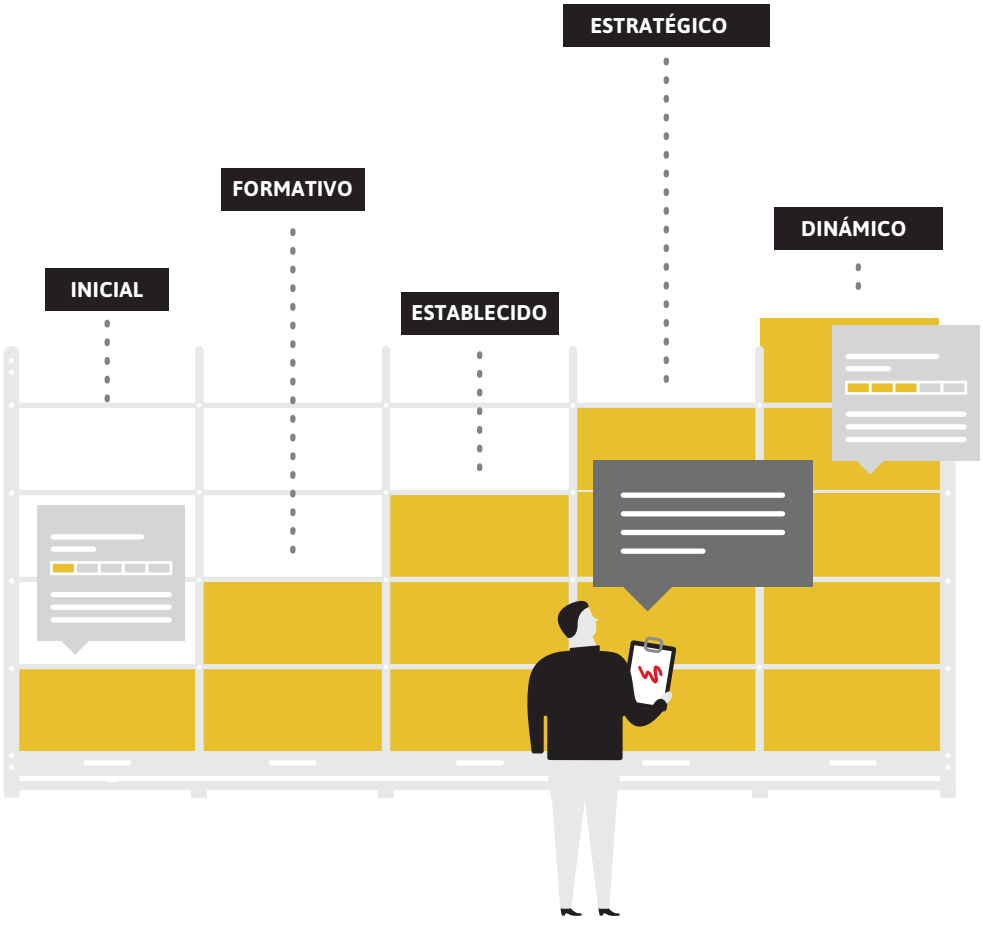
Protección de la Infraestructura Crítica Nacional (ICN)
Identificación
Organización
Planeación de respuesta
Coordinación
Gestión de riesgos

Gestión de crisis
Planeación
Evaluación

Redundancia digital
Planeación
Organización

Mercado de la ciberseguridad
Tecnologías de seguridad cibernética
Seguros de delincuencia cibernética

Niveles de madurez



Se han identificado cinco niveles de madurez de la capacidad de seguridad cibernética, de acuerdo con los cuales el más bajo implica un grado de capacidad más bien ad hoc, y el nivel más alto es tanto un enfoque estratégico como una capacidad de adaptarse dinámicamente o cambiar por consideraciones ambientales (operativas, amenazas, socio-técnicas y políticas).

INICIAL

En este nivel, o nada existe, o es de naturaleza muy embrionaria. También incluye un pensamiento o una observación acerca de un problema, pero no una acción.

FORMATIVO

Algunas características del subfactor han comenzado a crecer y ser formuladas, pero pueden ser casuales, desorganizadas, mal definidas o simplemente "nuevas".

ESTABLECIDO

Los elementos del subfactor están establecidos y funcionando. Sin embargo, no se ha considerado bien la asignación relativa de recursos. Ha habido poca toma de decisiones de compensación en relación con la inversión relativa en los distintos elementos del subfactor. Pero el subfactor es funcional y está definido.

ESTRATÉGICO

Estratégico no significa importante; más bien, se trata de una selección. Al nivel nacional se han elegido las partes del subfactor que son clave, así como aquellas que son menos importantes para la organización/país en particular. Estas elecciones toman en consideración un resultado esperado, una vez implementado, que contiene circunstancias particulares y otros objetivos nacionales existentes.

DINÁMICO

A nivel dinámico, existen mecanismos claros para alterar la estrategia en función de las circunstancias imperantes. Por ejemplo, la tecnología del entorno de amenazas, conflicto global, un cambio significativo en un área de interés (por ejemplo, la delincuencia cibernética o privacidad). Organizaciones dinámicas han desarrollado métodos para cambiar las estrategias, de acuerdo con una manera de "sentir y responder". La toma de decisiones rápida, la reasignación de los recursos y la atención constante a los cambios del entorno son las características de este nivel.

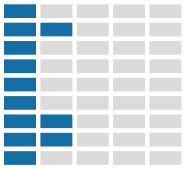
Perfiles de países

.ag

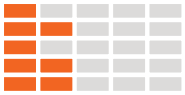
Antigua y Barbuda

Política y estrategia

Cultura y sociedad

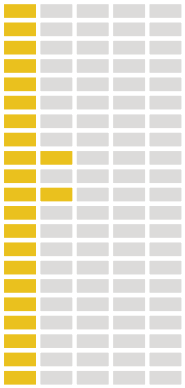


Educación



Marcos legales

Tecnología



En los últimos cuatro años el uso de Internet por parte de la población de Antigua y Barbuda se ha incrementado notablemente, del 47% al 64%[1]. Al contar con esta comunidad digital aún mayor, el Gobierno de Antigua y Barbuda ha comenzado a darle prioridad a la seguridad cibernética como una preocupación nacional[2]. Se están realizando consultas entre las partes interesadas para desarrollar una estrategia nacional de seguridad cibernética y un CSIRT nacional. Las responsabilidades informales de seguridad cibernética recaen bajo el Ministerio de Información, Difusión, Telecomunicaciones, Ciencia y Tecnología, mientras que la Organización Nacional de Políticas de Control de Drogas y Lavado de Activos sirve como el Punto Nacional de Contacto para organizaciones nacionales.

Los operadores de las infraestructuras críticas nacionales por lo general comprenden los riesgos de la seguridad cibernética y aplican ciertas tecnologías y estándares de seguridad para mejorar la resiliencia, aunque no exista una entidad designada para aplicar las normas de manera uniforme. Además, sin un mecanismo de respuesta de emergencias designado, el país no puede mantener información exacta sobre las amenazas a la seguridad cibernética y responder a eventos.

En 2013 el Gobierno aprobó tres leyes para complementar la Ley de Delitos de Transferencias Electrónicas de Fondos vigente (2006) y fortalecer el marco jurídico del país para las Tecnologías de Información y Comunicaciones (TIC): la Ley de Delitos Electrónicos, la Ley de Pruebas Electrónicas y la Ley de Protección de Datos. El Laboratorio de Investigación Cibernética Regional de la Policía Real de Antigua y Barbuda investiga el delito cibernético tanto a nivel nacional como en la región del Caribe. También procesa evidencia digital que se presentará en los casos de delitos cibernéticos. Sin embargo, Antigua y Barbuda no cuenta con un mecanismo de divulgación formal para el sector privado y son pocos los ataques cibernéticos que se denuncian a las autoridades. En ese sentido el Gobierno de Antigua y Barbuda también ha ratificado la Convención sobre los Derechos del Niño. Los artículos 16, 17 (e) y 34 (c) de la convención reconocen los derechos de los niños a ser protegidos de acciones maliciosas, incluyendo delincuencia cibernética y pornografía infantil.

El Ministerio de Información ha desarrollado planes para producir una campaña de sensibilización acerca de la seguridad cibernética en colaboración con la Iniciativa para Conectar Antigua y Barbuda. No hay ninguna campaña actualmente en curso. Las oportunidades de educación sobre seguridad cibernética en el país son limitadas, con excepción del Instituto Internacional de Tecnología de Antigua y Barbuda que ofrece cursos sobre el tema. Las empresas del sector privado se han vuelto cada vez más conscientes de los riesgos de seguridad cibernética y han comenzado a tomar iniciativas para capacitar a los empleados.

FUENTE DE ESTADÍSTICAS

Banco Mundial | Banco de datos,
Último acceso: noviembre de 2015.
databank.bancomundial.org/data/home.aspx

La fuente es la misma para todos los países.

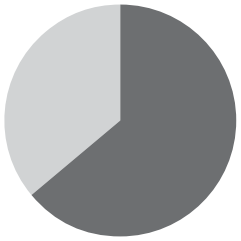
Personas con acceso a Internet*

Los usuarios de Internet son personas que han utilizado Internet (en cualquier lugar) en los últimos 12 meses. Internet puede ser utilizado a través de un ordenador, teléfono móvil, agenda electrónica, máquina de juegos, TV digital, etc.
Banco de Datos del Banco Mundial (2016).

POBLACIÓN TOTAL DEL PAÍS	**90.900**
Abonos a teléfonos celulares	109.100
Personas con acceso a Internet*	58.176

Penetración de Internet

64%



Política y estrategia

Estrategia nacional de seguridad cibernética oficial o documentada

- Desarrollo de la estrategia
- Organización
- Contenido

Defensa cibernética

- Estrategia
- Organización
- Coordinación

Cultura y sociedad

Mentalidad de seguridad cibernética

- En el gobierno
- En el sector privado
- En la sociedad

Conciencia de seguridad cibernética

- Sensibilización

Confianza en el uso de Internet

- En los servicios en línea
- En el gobierno electrónico
- En el comercio electrónico

Privacidad en línea

- Normas de privacidad
- Privacidad del empleado

Educación

Disponibilidad nacional de la educación y formación cibernéticas

- Educación
- Formación

Desarrollo nacional de la educación de seguridad cibernética

- Desarrollo nacional de la educación de seguridad cibernética

Formación e iniciativas educativas públicas y privadas

- Capacitación de empleados en seguridad cibernética

Gobernanza corporativa, conocimiento y normas

- Comprensión de la seguridad cibernética por parte de empresas privadas y estatales

Marcos legales

Marcos jurídicos de seguridad cibernética

- Para la seguridad de las TIC
- Privacidad, protección de datos y otros derechos humanos
- Derecho sustantivo de delincuencia cibernética
- Derecho procesal de delincuencia cibernética

Investigación jurídica

- Cumplimiento de la ley
- La fiscalía
- Tribunales

Divulgación responsable de la información

- Divulgación responsable de la información

Tecnologías

Adhesión a las normas

- Aplicación de las normas y prácticas mínimas aceptables
- Adquisiciones
- Desarrollo de softwre

Organizaciones de coordinación de seguridad cibernética

- Centro de mando y control
- Capacidad de respuesta a incidentes

Respuesta a incidentes

- Identificación y designación
- Organización
- Coordinación

Resiliencia de la infraestructura nacional

- Infraestructura tecnológica
- Resiliencia nacional

Protección de la Infraestructura Crítica Nacional (ICN)

- Identificación
- Organización
- Planeación de respuesta
- Coordinación
- Gestión de riesgos

Gestión de crisis

- Planeación
- Evaluación

Redundancia digital

- Planeación
- Organización

Mercado de la ciberseguridad

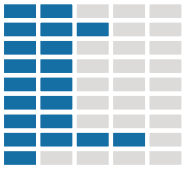
- Tecnologías de seguridad cibernética
- Seguros de delincuencia cibernética

.ar

Argentina

Política y estrategia

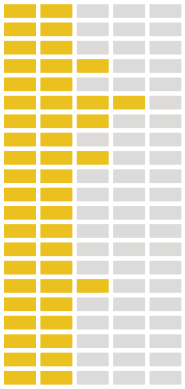
Cultura y sociedad



Educación

Marcos legales

Tecnología



Bajo la dirección del Programa Nacional de Infraestructuras Criticas de Información y Ciberseguridad (ICIC) y en coordinación con diversos organismos, instituciones académicas y el sector privado, el Gobierno de Argentina ha desarrollado un proyecto de Estrategia Nacional de Seguridad Cibernética que se encuentra en espera de adopción. Argentina se distingue por haber formado el primer CSIRT nacional en 1994, que desde 2011 ha funcionado bajo el ICIC. ICIC-CERT mantiene un registro central de los eventos y amenazas de seguridad cibernética. Las Fuerzas Armadas realizan Ejercicios Nacionales de Respuesta a Incidentes Cibernéticos (ENRIC) anuales para compartir mejores prácticas y revisar funciones de mando y control; sin embargo actualmente tienen una capacidad limitada de resiliencia cibernética.

Anteriormente la infraestructura crítica nacional (ICN) se manejaba más o menos de manera informal; sin embargo, en junio de 2015 la Presidencia de la República de Argentina emitió el Decreto n° 1067/2015 que reestructuró el control gubernamental de la ICN, y estableció una Oficina Nacional bajo la dirección de la Subsecretaría de Protección de Infraestructuras Críticas de Información y Ciberseguridad bajo la Jefatura del Gabinete de Ministros y Secretaría del Gabinete. Este nuevo programa trabajará para desarrollar normas y estándares de seguridad cibernética, así como para colaborar con el sector privado para mejorar la resiliencia de la ICN.

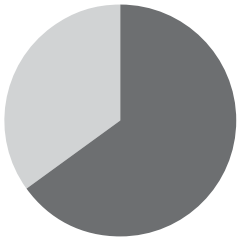
En medio de un aumento de los delitos informáticos, el Gobierno de Argentina ha construido un exhaustivo marco jurídico para las TIC, incluyendo la Ley 26.388, el Código Penal y la Ley 25.326 sobre protección de datos. También está desarrollando legislación procesal para el tratamiento de evidencia digital. Si bien existen mecanismos para la divulgación, el sector privado no está obligado por ley a reportar las violaciones a la seguridad cibernética. Sin embargo ha crecido de manera significativa entre las empresas una conciencia de riesgos de seguridad cibernética. La División de Delitos Tecnológicos de la Policía Federal Argentina (PFA) es responsable de investigar los casos de delitos informáticos y asume una serie de capacidades, que incluyen el suministro de información sobre cómo detectar y reportar ataques cibernéticos. Recientemente, el Gobierno de Argentina estableció también un punto focal en materia de ciberdelincuencia bajo la oficina del Ministerio Público Fiscal.

Como los servicios de gobierno electrónico y comercio electrónico de la Argentina continúan en expansión, las entidades gubernamentales han liderado campañas de concientización para educar al público sobre la seguridad cibernética. Dos ejemplos notables son "Internet Sano" del ICIC, que se centra en mejores prácticas para el uso seguro de Internet, y "Con Vos en la Web" bajo la dirección del Ministerio de Justicia y Derechos Humanos, que les enseña a niños y niñas, padres y maestros sobre la amenaza de la captación de menores en línea o grooming (creación de lazos de amistad abusivos en la web con los niños para atraerlos al abuso sexual o la trata de personas). Además, algunas universidades ofrecen programas de grado en seguridad cibernética e informática forense.

POBLACIÓN TOTAL DEL PAÍS	**42.980.026**
Abonos a teléfonos celulares	66.356.509
Personas con acceso a Internet	27.937.016

Penetración de Internet

65%



Política y estrategia

Estrategia nacional de seguridad cibernética oficial o documentada
Desarrollo de la estrategia
Organización
Contenido

Defensa cibernética
Estrategia
Organización
Coordinación

Cultura y sociedad

Mentalidad de seguridad cibernética
En el gobierno
En el sector privado
En la sociedad

Conciencia de seguridad cibernética
Sensibilización

Confianza en el uso de Internet
En los servicios en línea
En el gobierno electrónico
En el comercio electrónico

Privacidad en línea
Normas de privacidad
Privacidad del empleado

Educación

Disponibilidad nacional de la educación y formación cibernéticas
Educación
Formación

Desarrollo nacional de la educación de seguridad cibernética
Desarrollo nacional de la educación de seguridad cibernética

Formación e iniciativas educativas públicas y privadas
Capacitación de empleados en seguridad cibernética

Gobernanza corporativa, conocimiento y normas
Comprensión de la seguridad cibernética por parte de empresas privadas y estatales

Marcos legales

Marcos jurídicos de seguridad cibernética
Para la seguridad de las TIC
Privacidad, protección de datos y otros derechos humanos
Derecho sustantivo de delincuencia cibernética
Derecho procesal de delincuencia cibernética

Investigación jurídica
Cumplimiento de la ley
La fiscalía
Tribunales

Divulgación responsable de la información
Divulgación responsable de la información

Tecnologías

Adhesión a las normas
Aplicación de las normas y prácticas mínimas aceptables
Adquisiciones
Desarrollo de softwre

Organizaciones de coordinación de seguridad cibernética
Centro de mando y control
Capacidad de respuesta a incidentes

Respuesta a incidentes
Identificación y designación
Organización
Coordinación

Resiliencia de la infraestructura nacional
Infraestructura tecnológica
Resiliencia nacional

Protección de la Infraestructura Crítica Nacional (ICN)
Identificación
Organización
Planeación de respuesta
Coordinación
Gestión de riesgos

Gestión de crisis
Planeación
Evaluación

Redundancia digital
Planeación
Organización

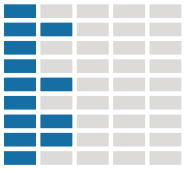
Mercado de la ciberseguridad
Tecnologías de seguridad cibernética
Seguros de delincuencia cibernética

.bs

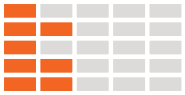
Bahamas (Commonwealth de)

Política y estrategia

Cultura y sociedad

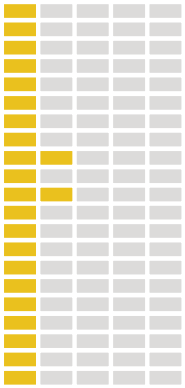


Educación



Marcos legales

Tecnología



El Ministerio de Seguridad Nacional del Gobierno de Bahamas es la principal entidad encargada de la seguridad cibernética en el país. Aunque no ha lanzado una política o estrategia nacional de seguridad cibernética, el 23 de abril de 2014 el Ministerio de Seguridad Nacional llevó a cabo un taller con múltiples partes interesadas y con el apoyo del Programa de Seguridad Cibernética de la OEA para el desarrollo de una estrategia nacional[3]. El Gobierno de Bahamas no cuenta con un CSIRT nacional para responder a eventos cibernéticos. Sin embargo tras un ataque en mayo de 2015 de un extremista islámico contra la infraestructura de TI del gobierno, se creó un grupo de trabajo de expertos y en junio de ese año se ofreció al personal del gobierno y del sector privado un curso gratuito de formación en hackeos éticos[4]. La infraestructura nacional de TI de Bahamas se gestiona de manera informal y no existe categorización formal de vulnerabilidades o amenazas.

En 2003 el Parlamento promulgó la Ley de Uso Indebido de Equipos de Cómputo, que dispone criminalización exhaustiva de y derecho procesal para ataques cibernéticos y actos maliciosos relacionados. El Parlamento también ha firmado la Ley de Protección de Datos (2003) y la Ley de Transacciones y Comunicaciones Electrónicas (2006) que protegen los derechos de los ciudadanos en la web y establecen normas y reglamentos para el comercio electrónico y otros servicios en línea respectivamente. Por otra parte, Bahamas se ha adherido a la Convención sobre los Derechos del Niño, que incluye la protección de los niños y niñas contra el abuso o la explotación en Internet.

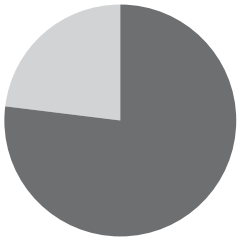
La Policía Real de Bahamas maneja los casos de delitos cibernéticos en el país y tiene previsto establecer una Unidad de Investigaciones de Delitos Cibernéticos específica, que aún no ha entrado en funcionamiento. Actualmente no existe ningún requisito de divulgación para el sector privado para denunciar violaciones a las autoridades. Por otra parte los tribunales y los fiscales cuentan con una capacidad limitada para manejar evidencia electrónica.

No hay ninguna campaña de sensibilización actualmente en Bahamas, pero sí hay algunas opciones disponibles para la formación en el tema, como el Programa de Certificación Avanzada de la International Compliance Association (ICA) en Seguridad Cibernética ofrecido en el Instituto de Servicios Financieros de Bahamas.

POBLACIÓN TOTAL DEL PAÍS	**383.054**
Abonos a teléfonos celulares	273.300
Personas con acceso a Internet	294.951

Penetración de Internet

77%



Política y estrategia

Estrategia nacional de seguridad cibernética oficial o documentada

- Desarrollo de la estrategia
- Organización
- Contenido

Defensa cibernética

- Estrategia
- Organización
- Coordinación

Cultura y sociedad

Mentalidad de seguridad cibernética

- En el gobierno
- En el sector privado
- En la sociedad

Conciencia de seguridad cibernética

- Sensibilización

Confianza en el uso de Internet

- En los servicios en línea
- En el gobierno electrónico
- En el comercio electrónico

Privacidad en línea

- Normas de privacidad
- Privacidad del empleado

Educación

Disponibilidad nacional de la educación y formación cibernéticas

- Educación
- Formación

Desarrollo nacional de la educación de seguridad cibernética

- Desarrollo nacional de la educación de seguridad cibernética

Formación e iniciativas educativas públicas y privadas

- Capacitación de empleados en seguridad cibernética

Gobernanza corporativa, conocimiento y normas

- Comprensión de la seguridad cibernética por parte de empresas privadas y estatales

Marcos legales

Marcos jurídicos de seguridad cibernética

- Para la seguridad de las TIC
- Privacidad, protección de datos y otros derechos humanos
- Derecho sustantivo de delincuencia cibernética
- Derecho procesal de delincuencia cibernética

Investigación jurídica

- Cumplimiento de la ley
- La fiscalía
- Tribunales

Divulgación responsable de la información

- Divulgación responsable de la información

Tecnologías

Adhesión a las normas

- Aplicación de las normas y prácticas mínimas aceptables
- Adquisiciones
- Desarrollo de softwre

Organizaciones de coordinación de seguridad cibernética

- Centro de mando y control
- Capacidad de respuesta a incidentes

Respuesta a incidentes

- Identificación y designación
- Organización
- Coordinación

Resiliencia de la infraestructura nacional

- Infraestructura tecnológica
- Resiliencia nacional

Protección de la Infraestructura Crítica Nacional (ICN)

- Identificación
- Organización
- Planeación de respuesta
- Coordinación
- Gestión de riesgos

Gestión de crisis

- Planeación
- Evaluación

Redundancia digital

- Planeación
- Organización

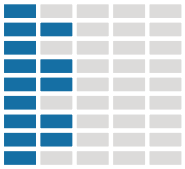
Mercado de la ciberseguridad

- Tecnologías de seguridad cibernética
- Seguros de delincuencia cibernética

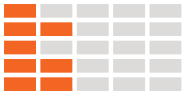
Barbados

Política y estrategia

Cultura y sociedad

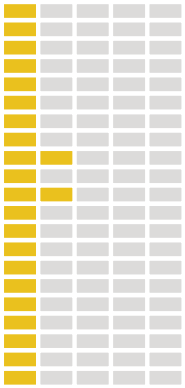


Educación



Marcos legales

Tecnología



En los últimos años el Gobierno de Barbados ha dado los primeros pasos para fortalecer la seguridad cibernética de su país. En 2013 la Unidad de Telecomunicaciones perteneciente al Ministerio de Energía firmó un acuerdo con la Unidad Internacional de Telecomunicaciones para establecer un CSIRT nacional y el gobierno se encuentra actualmente en conversaciones consultivas con la Unión de Telecomunicaciones del Caribe y la Organización de Telecomunicaciones del Commonwealth para desarrollar un "Modelo de Gobernanza Cibernética del Commonwealth". Sin embargo la aplicación de estas medidas ha sido lenta y las autoridades han mencionado como obstáculos para el avance la falta de fondos para la seguridad cibernética y una limitada cooperación interinstitucional.

En junio de 2015 la página web del Servicio de Información del Gobierno de Barbados fue atacada por piratas informáticos. Afortunadamente en cuestión de horas las autoridades pudieron restaurar el sitio web y mitigar el ataque[5]. Mientras que el sector bancario y algunas de las principales empresas han adoptado medidas de seguridad cibernética más fuertes, las autoridades creen que muchas empresas del sector privado y algunas entidades gubernamentales carecen de estructuras adecuadas para defenderse de las amenazas cibernéticas.

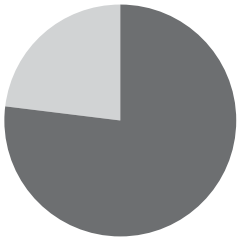
La Unidad de Delitos Cibernéticos de la Policía Real de Barbados es la principal agencia responsable de investigar los casos de delincuencia cibernética. La unidad recibe capacitación técnica de expertos regionales e internacionales en materia de seguridad cibernética y está trabajando para crear su propio laboratorio de análisis forense digital. En cuanto a los delitos informáticos, la Policía Real de Barbados cumple con la Ley de Uso Indebido de Equipos de Cómputo, 2005-4, que incluye tanto el derecho sustantivo como procesal para la investigación de la delincuencia cibernética. Barbados también ha promulgado la Ley de Asistencia Mutua en Asuntos Penales, Capítulo 140 Sección 6, que le permite al Gobierno de esta nación solicitar la ayuda de los países del Commonwealth en la obtención de pruebas electrónicas.

Tres cuartas partes de la población de Barbados está conectada a Internet y las partes interesadas en la seguridad cibernética están preocupadas por que la gran mayoría de la sociedad no es consciente de los riesgos y vulnerabilidades asociadas con el uso de tecnología de la información[6]. Para crear conciencia, Barbados se ha sumado a la campaña THINKCLICKSURF de la Unidad Internacional de Telecomunicaciones. Como parte de la campaña, la Policía Real de Barbados realiza una gira por las escuelas primarias y secundarias de todo el país para educar a los estudiantes sobre las prácticas seguras de Internet, la privacidad y el acoso en línea. En cuanto a la educación superior, el campus de la Universidad de las Indias Occidentales de Barbados ofrece cursos, pero en la actualidad no existe un programa de grado en seguridad cibernética.

POBLACIÓN TOTAL DEL PAÍS	**283.380**
Abonos a teléfonos celulares	305.456
Personas con acceso a Internet	218.202

Penetración de Internet

77%



Política y estrategia

Estrategia nacional de seguridad cibernética oficial o documentada

- Desarrollo de la estrategia
- Organización
- Contenido

Defensa cibernética

- Estrategia
- Organización
- Coordinación

Cultura y sociedad

Mentalidad de seguridad cibernética

- En el gobierno
- En el sector privado
- En la sociedad

Conciencia de seguridad cibernética

- Sensibilización

Confianza en el uso de Internet

- En los servicios en línea
- En el gobierno electrónico
- En el comercio electrónico

Privacidad en línea

- Normas de privacidad
- Privacidad del empleado

Educación

Disponibilidad nacional de la educación y formación cibernéticas

- Educación
- Formación

Desarrollo nacional de la educación de seguridad cibernética

- Desarrollo nacional de la educación de seguridad cibernética

Formación e iniciativas educativas públicas y privadas

- Capacitación de empleados en seguridad cibernética

Gobernanza corporativa, conocimiento y normas

- Comprensión de la seguridad cibernética por parte de empresas privadas y estatales

Marcos legales

Marcos jurídicos de seguridad cibernética

- Para la seguridad de las TIC
- Privacidad, protección de datos y otros derechos humanos
- Derecho sustantivo de delincuencia cibernética
- Derecho procesal de delincuencia cibernética

Investigación jurídica

- Cumplimiento de la ley
- La fiscalía
- Tribunales

Divulgación responsable de la información

- Divulgación responsable de la información

Tecnologías

Adhesión a las normas

- Aplicación de las normas y prácticas mínimas aceptables
- Adquisiciones
- Desarrollo de softwre

Organizaciones de coordinación de seguridad cibernética

- Centro de mando y control
- Capacidad de respuesta a incidentes

Respuesta a incidentes

- Identificación y designación
- Organización
- Coordinación

Resiliencia de la infraestructura nacional

- Infraestructura tecnológica
- Resiliencia nacional

Protección de la Infraestructura Crítica Nacional (ICN)

- Identificación
- Organización
- Planeación de respuesta
- Coordinación
- Gestión de riesgos

Gestión de crisis

- Planeación
- Evaluación

Redundancia digital

- Planeación
- Organización

Mercado de la ciberseguridad

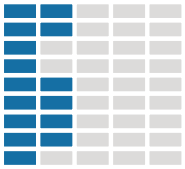
- Tecnologías de seguridad cibernética
- Seguros de delincuencia cibernética

.bz

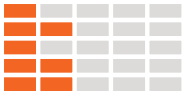
Belice

Política y estrategia

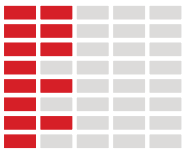
Cultura y sociedad



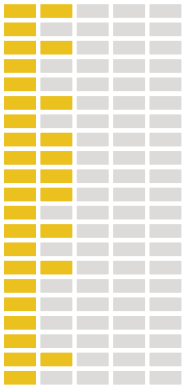
Educación



Marcos legales



Tecnología



En 2014 el Ministerio de Seguridad Nacional organizó un Comité ad hoc de Seguridad Cibernética, compuesto por múltiples partes interesadas, incluyendo la academia y el sector privado, para trabajar juntos en el desarrollo de una estrategia nacional de seguridad cibernética, reforzar la legislación de delito cibernético y crear conciencia sobre el delito cibernético en Belice. El comité ha recibido asistencia del Programa de Seguridad Cibernética de la OEA. Además Belice está planeando una Política Nacional de Innovación de las TIC que busca ampliar los servicios de gobierno electrónico, así como implementar medidas de seguridad cibernética relacionadas. Adicionalmente la Organización Central de Tecnologías de Información también está concluyendo su Política, Estrategia y Plan de Acción de Gobierno Electrónico. El país también participa en el Proyecto de la Unión de Telecomunicaciones del Caribe y la Comunidad del Caribe (CARICOM) HIPCAR, una iniciativa para unificar las gestiones de innovación de las TIC en toda la región.

Belice no cuenta ni con una política de defensa cibernética ni un CSIRT nacional; en consecuencia los ataques cibernéticos son manejados principalmente por la Unidad de TI del Departamento de Policía del país. La Unidad de TI del Departamento de Policía proporcionó apoyo notable en seguridad cibernética en coordinación con CARICOM para la Copa Mundial de Cricket de 2007 y se comunica regularmente con los CSIRT regionales. Belice ha promulgado cuatro leyes relacionadas con la delincuencia cibernética, a saber: Ley de Telecomunicaciones, Ley de Pruebas Electrónicas, Ley de Propiedad Intelectual y Ley de Interceptación de Comunicaciones. Sin embargo, sin una ley penal integral la policía y el Poder Judicial tienen dificultades para enjuiciar efectivamente los delitos cibernéticos. En consecuencia, aunque no existe un acuerdo vinculante para la divulgación de brechas en seguridad cibernética, el gobierno y sector privado cooperan para denunciar y abordar los ataques cibernéticos y, si bien las estadísticas son limitadas, el Gobierno de Belice ha notado un aumento de los incidentes en los últimos años.

En respuesta a las crecientes amenazas a la seguridad cibernética en la región, el gobierno ha comenzado a promover tecnología y estándares más fuertes de seguridad entre las entidades y los operadores de la Infraestructura Crítica Nacional (ICN). Sin embargo, las partes interesadas no han formulado planes de respuesta u otras políticas de gestión de crisis en relación con la protección de la ICN.

Con una penetración de Internet del 39%, gran parte de la sociedad de Belice no ha desarrollado una mentalidad frente a la seguridad cibernética[7]. Con el fin de crear conciencia sobre los asuntos de seguridad cibernética, el Departamento de Policía de Belice (BPD, por sus siglas en inglés) participa en un "Programa Itinerante de Tecnologías de Información y Comunicaciones" anual, organizado por el Ministerio de Energía, Ciencia y Tecnología y Servicios Públicos. El BPD utiliza esta plataforma para educar a las comunidades sobre las oportunidades y los riesgos del espacio cibernético. El próximo año, con el apoyo del sector privado, la academia y otras partes interesadas, el Gobierno de Belice tiene previsto celebrar su Primera Semana Anual de Seguridad Cibernética. Además, Belice también espera lanzar la campaña de educación pública STOP.THINK.CONNECT. para finales de 2015. Actualmente no hay programas de licenciatura en seguridad cibernética en las universidades del país, pero algunas empresas del sector privado sí ofrecen programas de formación.

POBLACIÓN TOTAL DEL PAÍS	**351.706**
Abonos a teléfonos celulares	172.300
Personas con acceso a Internet	137.165

Penetración de Internet

39%

Política y estrategia

Estrategia nacional de seguridad cibernética oficial o documentada

- Desarrollo de la estrategia
- Organización
- Contenido

Defensa cibernética

- Estrategia
- Organización
- Coordinación

Cultura y sociedad

Mentalidad de seguridad cibernética

- En el gobierno
- En el sector privado
- En la sociedad

Conciencia de seguridad cibernética

- Sensibilización

Confianza en el uso de Internet

- En los servicios en línea
- En el gobierno electrónico
- En el comercio electrónico

Privacidad en línea

- Normas de privacidad
- Privacidad del empleado

Educación

Disponibilidad nacional de la educación y formación cibernéticas

- Educación
- Formación

Desarrollo nacional de la educación de seguridad cibernética

- Desarrollo nacional de la educación de seguridad cibernética

Formación e iniciativas educativas públicas y privadas

- Capacitación de empleados en seguridad cibernética

Gobernanza corporativa, conocimiento y normas

- Comprensión de la seguridad cibernética por parte de empresas privadas y estatales

Marcos legales

Marcos jurídicos de seguridad cibernética

- Para la seguridad de las TIC
- Privacidad, protección de datos y otros derechos humanos
- Derecho sustantivo de delincuencia cibernética
- Derecho procesal de delincuencia cibernética

Investigación jurídica

- Cumplimiento de la ley
- La fiscalía
- Tribunales

Divulgación responsable de la información

- Divulgación responsable de la información

Tecnologías

Adhesión a las normas

- Aplicación de las normas y prácticas mínimas aceptables
- Adquisiciones
- Desarrollo de softwre

Organizaciones de coordinación de seguridad cibernética

- Centro de mando y control
- Capacidad de respuesta a incidentes

Respuesta a incidentes

- Identificación y designación
- Organización
- Coordinación

Resiliencia de la infraestructura nacional

- Infraestructura tecnológica
- Resiliencia nacional

Protección de la Infraestructura Crítica Nacional (ICN)

- Identificación
- Organización
- Planeación de respuesta
- Coordinación
- Gestión de riesgos

Gestión de crisis

- Planeación
- Evaluación

Redundancia digital

- Planeación
- Organización

Mercado de la ciberseguridad

- Tecnologías de seguridad cibernética
- Seguros de delincuencia cibernética

Bolivia

Política y estrategia

Cultura y sociedad

Educación

Marcos legales

Tecnología

La Agencia para el Desarrollo de la Sociedad de la Información en Bolivia (ADSIB) es la agencia principal de gestión de asuntos de seguridad cibernética y gobierno electrónico en Bolivia. Los objetivos del ADSIB incluyen gestiones de coordinación para ampliar las Tecnologías de Información y Comunicaciones (TIC) mediante la sensibilización de la sociedad sobre la seguridad cibernética y la asociación en proyectos con el sector privado y la sociedad civil[8]. El Gobierno de Bolivia no ha desarrollado una estrategia o política de seguridad cibernética oficial. Además, previamente tuvo que coordinar la respuesta a incidentes a través de los CSIRT de otros países, por ejemplo frente a una amenaza a la Infraestructura Crítica Nacional a través del ArCERT de Argentina. Sin embargo, en 2015 se puso en operación el CSIRT oficial de Bolivia, CSIRT-BO.

En 2013 Bolivia fortaleció su infraestructura nacional de TI con el desarrollo de un Punto de Intercambio de Tráfico de Internet nacional (IXP), llamado PIT-BOLIVIA.[9] Los operadores de infraestructura crítica también han implementado procedimientos y estándares de seguridad ad hoc pero no existe una colaboración formal entre las partes interesadas en este sentido.

La División Informática Forense del Instituto de Investigaciones Técnico Científicas de la Universidad Policial (IITCUP) se encarga de los casos nacionales de delincuencia cibernética. El Gobierno ha estado trabajando recientemente para fortalecer la capacidad del IITCUP. La División hace cumplir el Capítulo XI del Código Penal (establecido en 1997), que tipifica como delito la manipulación o la obtención ilegal de información en Internet y en los artículos 253 y 254 del Código de Procedimiento Penal se establecen normas para la obtención de evidencia electrónica. La Asamblea Legislativa Plurinacional también ha aprobado el artículo 281 de la Ley 3325 de 2006 contra la trata de personas, la pornografía infantil y otros actos infames que a menudo se relacionan con Internet. No existe ninguna legislación específica relativa a la delincuencia informática. Sin embargo, el país ha desarrollado un proyecto de ley sobre documentos electrónicos, firma electrónica y comercio electrónico destinado a mejorar la capacidad de resiliencia de la infraestructura de TI y fortalecer la seguridad cibernética nacional. El IITCUP menciona la falta de un canal formal para la obtención de la divulgación oportuna de ataques cibernéticos como un problema importante para hacer cumplir la ley.

Mientras que el ADSIB ofrece una variedad de literatura que detalla el uso seguro de Internet en su sitio web, así como seminarios de formación, hasta la fecha el Gobierno de Bolivia no ha liderado ninguna campaña nacional de sensibilización sobre la materia. En cambio, muchas universidades ofrecen clases sobre seguridad cibernética, aunque en su mayoría son a nivel teórico con trabajo práctico técnico limitado.

POBLACIÓN TOTAL DEL PAÍS	**10.561.887**
Abonos a teléfonos celulares	10.450.341
Personas con acceso a Internet	4.119.136

Penetración de Internet

39%

Política y estrategia

Estrategia nacional de seguridad cibernética oficial o documentada

- Desarrollo de la estrategia
- Organización
- Contenido

Defensa cibernética

- Estrategia
- Organización
- Coordinación

Cultura y sociedad

Mentalidad de seguridad cibernética

- En el gobierno
- En el sector privado
- En la sociedad

Conciencia de seguridad cibernética

- Sensibilización

Confianza en el uso de Internet

- En los servicios en línea
- En el gobierno electrónico
- En el comercio electrónico

Privacidad en línea

- Normas de privacidad
- Privacidad del empleado

Educación

Disponibilidad nacional de la educación y formación cibernéticas

- Educación
- Formación

Desarrollo nacional de la educación de seguridad cibernética

- Desarrollo nacional de la educación de seguridad cibernética

Formación e iniciativas educativas públicas y privadas

- Capacitación de empleados en seguridad cibernética

Gobernanza corporativa, conocimiento y normas

- Comprensión de la seguridad cibernética por parte de empresas privadas y estatales

Marcos legales

Marcos jurídicos de seguridad cibernética

- Para la seguridad de las TIC
- Privacidad, protección de datos y otros derechos humanos
- Derecho sustantivo de delincuencia cibernética
- Derecho procesal de delincuencia cibernética

Investigación jurídica

- Cumplimiento de la ley
- La fiscalía
- Tribunales

Divulgación responsable de la información

- Divulgación responsable de la información

Tecnologías

Adhesión a las normas

- Aplicación de las normas y prácticas mínimas aceptables
- Adquisiciones
- Desarrollo de softwre

Organizaciones de coordinación de seguridad cibernética

- Centro de mando y control
- Capacidad de respuesta a incidentes

Respuesta a incidentes

- Identificación y designación
- Organización
- Coordinación

Resiliencia de la infraestructura nacional

- Infraestructura tecnológica
- Resiliencia nacional

Protección de la Infraestructura Crítica Nacional (ICN)

- Identificación
- Organización
- Planeación de respuesta
- Coordinación
- Gestión de riesgos

Gestión de crisis

- Planeación
- Evaluación

Redundancia digital

- Planeación
- Organización

Mercado de la ciberseguridad

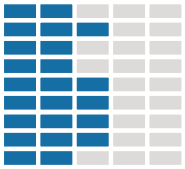
- Tecnologías de seguridad cibernética
- Seguros de delincuencia cibernética

.br

Brasil

Política y estrategia

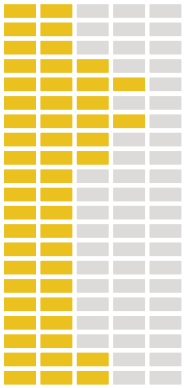
Cultura y sociedad



Educación

Marcos legales

Tecnología



Brasil ha realizado grandes inversiones en las TIC como una manera de promover el crecimiento económico y el progreso social. A la luz de su creciente adopción de las TIC, Brasil se ha convertido en un objetivo prioritario de los ataques y delitos cibernéticos incluyendo olas de phishing focalizado, malware y ataques DDoS antes de la Copa del Mundo de 2014. Mientras se prepara para los Juegos Olímpicos de 2016 la administración Río de Janeiro ha construido un centro urbano integrado.[10]

En 2010 el Departamento de Seguridad de la Información y Comunicaciones publicó la Guía de Referencia para la Protección de Infraestructuras Críticas de Información y el Libro Verde de Seguridad Cibernética en Brasil. Estos documentos han servido como base para la recién publicada Estrategia Nacional de Seguridad de las Comunicaciones de Información y Seguridad Cibernética de la Administración Pública Federal[11]. Las Fuerzas Armadas brasileñas también discuten las preocupaciones sobre defensa cibernética en su Libro Blanco de Defensa Nacional 2012. Recientemente crearon un Comando de Defensa Cibernética formal y una Escuela Nacional de Defensa Cibernética, además del Centro para la Defensa Cibernética del Ejército (CDCiber).

Brasil tiene varios de Equipos de Respuesta a Incidentes de Seguridad Informática (CSIRT), que van desde entidades administradas por el gobierno a equipos del sector privado o académicos. El Comité Gestor de Internet en Brasil (CGI.br) es el encargado de coordinar todas las iniciativas de servicios de Internet en el país y el Centro de Información de la Red Brasileña (NIC.br) trabaja para implementar este tipo de iniciativas[12]. El equipo Nacional de Respuesta a Incidentes Informáticos de Brasil (CERT.BR), que opera bajo el CGI.br y el NIC.br, es responsable de la respuesta y coordinación a incidentes, capacitación y campañas de concientización. El Departamento de Seguridad de Información y Comunicaciones de Brasil también mantiene un CSIRT, el CTIR.gov, que proporciona servicios de respuesta a incidentes y recopilación de datos para la Administración Pública Federal.

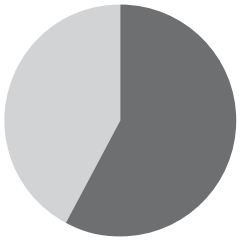
El esquema de Brasil para abordar las actividades cibernéticas ilícitas se basa en la Ley n° 12.965/2014, el "Marco de Derechos Civiles para Internet" y la Ley n° 12.737, que tipifica formalmente el delito cibernético. Sin embargo estas leyes se consideran insuficientes para disuadir a los delincuentes. Ha estado recientemente bajo consulta pública una ley específica para hacer frente a la privacidad en Internet y regular la conservación de datos por parte de los Proveedores de Servicios de Internet, pero no se ha adoptado formalmente. La Oficina para la Represión de la Delincuencia Cibernética de la Policía Federal es la principal entidad encargada de investigar los delitos cibernéticos y cuenta con un laboratorio forense digital. Algunos estados de Brasil también cuentan con equipos de enjuiciamiento especializados. Aunque el sector privado no está obligado a revelar incidentes cibernéticos, la Oficina para la Represión de la Delincuencia Cibernética tiene una relación laboral con las empresas.

La comprensión pública de los problemas de seguridad cibernética en Brasil es generalmente baja y organizaciones como el CGI.br y el NIC.br han tratado de abordarla mediante la emisión de numerosos boletines y campañas de sensibilización. El sector privado está cada vez más informado acerca de la necesidad de tener una mejor protección contra las amenazas cibernéticas. Las empresas y los operadores de infraestructuras críticas han implementado requisitos de privacidad para sus empleados y están desarrollando estándares de adquisiciones y tecnología. También existe un fuerte mercado nacional de tecnologías de seguridad cibernética. La academia ofrece una gran cantidad de oportunidades para la educación en seguridad cibernética con varias universidades que tienen programas de maestría y doctorado.

POBLACIÓN TOTAL DEL PAÍS	**206.077.898**
Abonos a teléfonos celulares	280.728.796
Personas con acceso a Internet	119.525.181

Penetración de Internet

58%



Política y estrategia

Estrategia nacional de seguridad cibernética oficial o documentada

- Desarrollo de la estrategia
- Organización
- Contenido

Defensa cibernética

- Estrategia
- Organización
- Coordinación

Cultura y sociedad

Mentalidad de seguridad cibernética

- En el gobierno
- En el sector privado
- En la sociedad

Conciencia de seguridad cibernética

- Sensibilización

Confianza en el uso de Internet

- En los servicios en línea
- En el gobierno electrónico
- En el comercio electrónico

Privacidad en línea

- Normas de privacidad
- Privacidad del empleado

Educación

Disponibilidad nacional de la educación y formación cibernéticas

- Educación
- Formación

Desarrollo nacional de la educación de seguridad cibernética

- Desarrollo nacional de la educación de seguridad cibernética

Formación e iniciativas educativas públicas y privadas

- Capacitación de empleados en seguridad cibernética

Gobernanza corporativa, conocimiento y normas

- Comprensión de la seguridad cibernética por parte de empresas privadas y estatales

Marcos legales

Marcos jurídicos de seguridad cibernética

- Para la seguridad de las TIC
- Privacidad, protección de datos y otros derechos humanos
- Derecho sustantivo de delincuencia cibernética
- Derecho procesal de delincuencia cibernética

Investigación jurídica

- Cumplimiento de la ley
- La fiscalía
- Tribunales

Divulgación responsable de la información

- Divulgación responsable de la información

Tecnologías

Adhesión a las normas

- Aplicación de las normas y prácticas mínimas aceptables
- Adquisiciones
- Desarrollo de softwre

Organizaciones de coordinación de seguridad cibernética

- Centro de mando y control
- Capacidad de respuesta a incidentes

Respuesta a incidentes

- Identificación y designación
- Organización
- Coordinación

Resiliencia de la infraestructura nacional

- Infraestructura tecnológica
- Resiliencia nacional

Protección de la Infraestructura Crítica Nacional (ICN)

- Identificación
- Organización
- Planeación de respuesta
- Coordinación
- Gestión de riesgos

Gestión de crisis

- Planeación
- Evaluación

Redundancia digital

- Planeación
- Organización

Mercado de la ciberseguridad

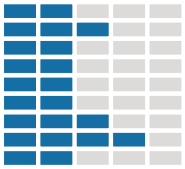
- Tecnologías de seguridad cibernética
- Seguros de delincuencia cibernética

.cl

Chile

Política y estrategia

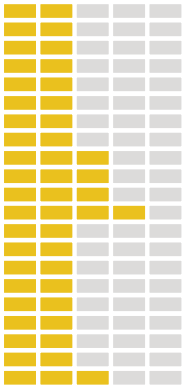
Cultura y sociedad



Educación

Marcos legales

Tecnología



El Ministerio del Interior y Seguridad Pública, el Secretario General de la Presidencia y la Subsecretaría de Telecomunicaciones son los principales organismos nacionales que establecen la política de seguridad cibernética a nivel gubernamental. Si bien el país no ha emitido una estrategia nacional de seguridad cibernética, la sensibilización entre las instituciones gubernamentales es generalizada. La infraestructura gubernamental presenta tecnología de seguridad actualizada y las partes interesadas pertinentes regularmente analizan los activos y vulnerabilidades de la Infraestructura Crítica Nacional. El Estado también coordina la planeación de gestión de crisis y ha puesto en marcha medidas de redundancia.

Las ramas de las Fuerzas Armadas de Chile comparten responsabilidades de defensa cibernética e información pero no tienen una estructura central de mando y control. Uno de los principales desafíos de Chile de cara al futuro es el fortalecimiento de su capacidad de respuesta a incidentes: el CSIRT-CL que se encuentra en funcionamiento desde 2004 ofrece respuesta a incidentes para los sitios web del gobierno pero no está institucionalizado formalmente a nivel nacional para abordar todo tipo de violaciones.

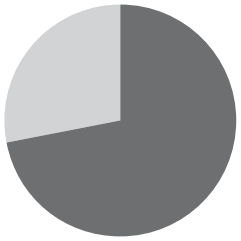
Chile ha establecido un marco jurídico global para hacer frente a los delitos cibernéticos. El Decreto Supremo n° 1299 describe las normas y define los roles para el manejo de la delincuencia cibernética, la Ley n° 19.223 introduce los delitos informáticos al Código Penal y la Ley n° 19.628 cubre la privacidad y protección de datos. Aunque el sector privado no está obligado por ley a divulgar las violaciones, el gobierno trabaja en estrecha colaboración con las empresas para informar y responder a incidentes cibernéticos. De acuerdo con las autoridades de Chile, la suplantación de identidad (phishing), malware y piratería informática son los tipos más frecuentes de ataques cibernéticos en el país. El Departamento de Investigación de Organizaciones Criminales (OS-9) y el Laboratorio de Criminalística de los Carabineros (LABOCAR), la policía nacional de Chile, llevan a cabo investigaciones y análisis forense digital respectivamente. Estas unidades han detenido con éxito numerosos criminales cibernéticos en los últimos años. Por último, los tribunales tienen una capacidad adecuada para manejar evidencia electrónica.

La mentalidad de seguridad cibernética es inconsistente en la sociedad chilena. En 2013, para crear conciencia, el Ministerio de Educación inició la campaña de Internet Segura para educar a los jóvenes sobre la privacidad y el uso seguro de Internet. También está en marcha una campaña, llamada Consumidor Digital, para que los ciudadanos tengan cuidado de los riesgos del comercio electrónico y para que entiendan sus derechos como consumidores. La Universidad de Chile ofrece títulos avanzados en seguridad cibernética y también están disponibles diversos cursos en línea y capacitación para empleados. Comparativamente, el sector privado se ha vuelto cada vez más consciente de los riesgos de seguridad cibernética y ha puesto en marcha planes para abordarlos.

POBLACIÓN TOTAL DEL PAÍS	**17.762.647**
Abonos a teléfonos celulares	23.683.351
Personas con acceso a Internet	12.789.105

Penetración de Internet

72%



Política y estrategia

Estrategia nacional de seguridad cibernética oficial o documentada

- Desarrollo de la estrategia
- Organización
- Contenido

Defensa cibernética

- Estrategia
- Organización
- Coordinación

Cultura y sociedad

Mentalidad de seguridad cibernética

- En el gobierno
- En el sector privado
- En la sociedad

Conciencia de seguridad cibernética

- Sensibilización

Confianza en el uso de Internet

- En los servicios en línea
- En el gobierno electrónico
- En el comercio electrónico

Privacidad en línea

- Normas de privacidad
- Privacidad del empleado

Educación

Disponibilidad nacional de la educación y formación cibernéticas

- Educación
- Formación

Desarrollo nacional de la educación de seguridad cibernética

- Desarrollo nacional de la educación de seguridad cibernética

Formación e iniciativas educativas públicas y privadas

- Capacitación de empleados en seguridad cibernética

Gobernanza corporativa, conocimiento y normas

- Comprensión de la seguridad cibernética por parte de empresas privadas y estatales

Marcos legales

Marcos jurídicos de seguridad cibernética

- Para la seguridad de las TIC
- Privacidad, protección de datos y otros derechos humanos
- Derecho sustantivo de delincuencia cibernética
- Derecho procesal de delincuencia cibernética

Investigación jurídica

- Cumplimiento de la ley
- La fiscalía
- Tribunales

Divulgación responsable de la información

- Divulgación responsable de la información

Tecnologías

Adhesión a las normas

- Aplicación de las normas y prácticas mínimas aceptables
- Adquisiciones
- Desarrollo de softwre

Organizaciones de coordinación de seguridad cibernética

- Centro de mando y control
- Capacidad de respuesta a incidentes

Respuesta a incidentes

- Identificación y designación
- Organización
- Coordinación

Resiliencia de la infraestructura nacional

- Infraestructura tecnológica
- Resiliencia nacional

Protección de la Infraestructura Crítica Nacional (ICN)

- Identificación
- Organización
- Planeación de respuesta
- Coordinación
- Gestión de riesgos

Gestión de crisis

- Planeación
- Evaluación

Redundancia digital

- Planeación
- Organización

Mercado de la ciberseguridad

- Tecnologías de seguridad cibernética
- Seguros de delincuencia cibernética

.co

Colombia

Política y estrategia

Cultura y sociedad

Educación

Marcos legales

Tecnología

El Consejo Nacional de Política Económica y Social del Gobierno de Colombia estableció la política nacional de seguridad cibernética CONPES 3701 bajo el auspicio del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), el Ministerio de Defensa, el Departamento Nacional de Planeación y otras instituciones nacionales clave. Además, en 2014 una Misión de Asistencia Técnica de la OEA al país ayudó a construir la capacidad de las partes interesadas de desarrollar marcos y políticas institucionales. Si bien está muy extendida la conciencia sobre el CONPES 3701, no se han definido claramente mandatos específicos. El Grupo de Respuesta de Emergencias Cibernéticas de Colombia (ColCERT) es una institución clave en defensa y seguridad cibernética y se muestra competente para la coordinación con otros organismos y el sector privado. El programa CERT de Colombia funciona principalmente como un mecanismo de respuesta a incidentes cibernéticos específicos de la organización, y los programas de gestión del riesgo han comenzado a surtir efecto. Últimamente, el Ministro de TIC de Colombia ha informado que una nueva estrategia de seguridad cibernética y defensa cibernética estará lista para finales de 2015 o inicios de 2016.

Colombia ha aprobado una legislación procesal penal integral y de efectiva penalización (Ley 1273 y Ley 906) para abordar los delitos cibernéticos y reconoce los tratados internacionales con Interpol y Europol. Las fuerzas del orden y el Poder Judicial tienen la capacidad de investigar y manejar casos de delincuencia cibernética, pero carecen de la formación y capacidad para lograr los mismos resultados en los tribunales. Asimismo, si bien la Ley 1581 establece un marco básico para la protección de datos y divulgación y denuncia de las violaciones de seguridad, a menudo los casos de los sectores público y privado no se informan.

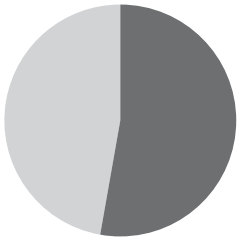
La conciencia social sobre la importancia de la privacidad y la seguridad en Internet y la confianza en los sistemas digitales del país ha crecido notablemente, en parte debido a las campañas nacionales, como en la campaña "en TIC Confío" del MinTIC. Colombia cuenta con más de 2.000 oportunidades de comercio electrónico y servicios de gobierno electrónico que se realizan en su mayoría en un entorno seguro. Aun así, la mayoría de ciudadanos y empleados privados cuentan con por lo menos un nivel mínimo de infraestructura de privacidad y hay leyes en vigor que obligan a las empresas a implementar políticas de protección de datos en el lugar de trabajo como la Ley 1581 de 2012 y el Decreto 1377 de 2013.

El desarrollo de educación de seguridad cibernética nacional ha experimentado un crecimiento notable y los foros público-privados y centros de excelencia financiados por el gobierno han comenzado a gestarse en el país. Numerosas universidades, organismos policiales y de defensa y las empresas privadas ofrecen cursos y capacitaciones, incluyendo maestrías y programas de acreditación.

POBLACIÓN TOTAL DEL PAÍS	**47.791.393**
Abonos a teléfonos celulares	55.330.727
Personas con acceso a Internet	25.329.438

Penetración de Internet

53%



Política y estrategia

Estrategia nacional de seguridad cibernética oficial o documentada

- Desarrollo de la estrategia
- Organización
- Contenido

Defensa cibernética

- Estrategia
- Organización
- Coordinación

Cultura y sociedad

Mentalidad de seguridad cibernética

- En el gobierno
- En el sector privado
- En la sociedad

Conciencia de seguridad cibernética

- Sensibilización

Confianza en el uso de Internet

- En los servicios en línea
- En el gobierno electrónico
- En el comercio electrónico

Privacidad en línea

- Normas de privacidad
- Privacidad del empleado

Educación

Disponibilidad nacional de la educación y formación cibernéticas

- Educación
- Formación

Desarrollo nacional de la educación de seguridad cibernética

- Desarrollo nacional de la educación de seguridad cibernética

Formación e iniciativas educativas públicas y privadas

- Capacitación de empleados en seguridad cibernética

Gobernanza corporativa, conocimiento y normas

- Comprensión de la seguridad cibernética por parte de empresas privadas y estatales

Marcos legales

Marcos jurídicos de seguridad cibernética

- Para la seguridad de las TIC
- Privacidad, protección de datos y otros derechos humanos
- Derecho sustantivo de delincuencia cibernética
- Derecho procesal de delincuencia cibernética

Investigación jurídica

- Cumplimiento de la ley
- La fiscalía
- Tribunales

Divulgación responsable de la información

- Divulgación responsable de la información

Tecnologías

Adhesión a las normas

- Aplicación de las normas y prácticas mínimas aceptables
- Adquisiciones
- Desarrollo de softwre

Organizaciones de coordinación de seguridad cibernética

- Centro de mando y control
- Capacidad de respuesta a incidentes

Respuesta a incidentes

- Identificación y designación
- Organización
- Coordinación

Resiliencia de la infraestructura nacional

- Infraestructura tecnológica
- Resiliencia nacional

Protección de la Infraestructura Crítica Nacional (ICN)

- Identificación
- Organización
- Planeación de respuesta
- Coordinación
- Gestión de riesgos

Gestión de crisis

- Planeación
- Evaluación

Redundancia digital

- Planeación
- Organización

Mercado de la ciberseguridad

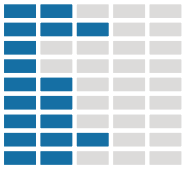
- Tecnologías de seguridad cibernética
- Seguros de delincuencia cibernética

.cr

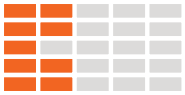
Costa Rica

Política y estrategia

Cultura y sociedad

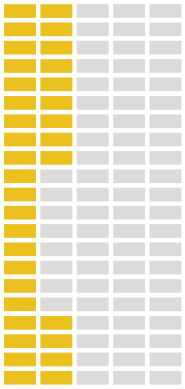


Educación



Marcos legales

Tecnología



El Ministerio de Ciencia, Tecnología y Telecomunicaciones (MICITT) de Costa Rica es la autoridad principal responsable del manejo de los problemas y del desarrollo de políticas relacionadas con la seguridad cibernética nacional. Otras instituciones, incluida la Secretaría Digital/ Gobierno Digital, la Sección de Delitos Informáticos del Poder Judicial, la Superintendencia de Telecomunicaciones, el Banco Central y la Agencia de Protección de Datos de los Habitantes (Prodhab), también han sido clave en esta área. El MICITT está en las etapas iniciales de la planificación de una estrategia de seguridad cibernética nacional.

El año 2012 fue un año decisivo para la seguridad cibernética en Costa Rica con la aprobación de la Ley 9048 que introdujo formalmente el delito cibernético al código penal del país. Costa Rica también reconoce la Convención Interamericana sobre Asistencia Mutua en Materia Penal (comúnmente conocida como la "Convención de Nassau") y regularmente coordina con la Interpol. Los ciudadanos en general gozan de la protección de la libertad de expresión y los derechos a la privacidad bajo la jurisdicción interna. Sin embargo, aunque la Fuerza Pública maneja un laboratorio forense digital, las autoridades judiciales tienen dificultades para procesar eficazmente los casos de delitos informáticos ya que un número limitado de fiscales y jueces tienen la capacidad de preparar y manejar casos que involucran evidencia electrónica.

Además, en 2012 el Gobierno de Costa Rica estableció el CSIRT-CR (bajo el MICITT). El CSIRT-CR es el organismo nacional encargado no solo de la tarea de responder a los trastornos de la seguridad cibernética, sino también de coordinar las funciones nacionales de mando y control. La entidad ha recibido asistencia técnica de la OEA y de otros expertos regionales e internacionales y ha detectado y mitigado con éxito las principales amenazas de seguridad cibernética, sobre todo un ataque DoS en 2013 al Instituto Costarricense de Electricidad (ICE) originado en Rusia. Actualmente no existe un registro público de incidentes, aunque el gobierno está en el proceso de desarrollar uno. Costa Rica no tiene un ejército permanente y la Fuerza Pública tiene estructuras y capacidades limitadas para construir capacidad de resiliencia cibernética.

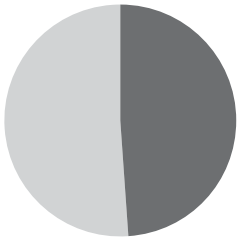
El sector público y las organizaciones de la infraestructura critica nacional han asumido y promovido normas de seguridad internacionales como la ISO/IEC 27001 pero el sector privado aún no las ha seguido y la falta de normas claras para el registro proveedores del servicio de Internet continúa retrasando el avance de la seguridad cibernética. Sin embargo, grupos como el ICE han presionado para tener estándares de desarrollo de software y el sector privado participa en el mercado de la seguridad informática, mediante la inversión en sistemas de control de tecnología de la información y la discusión de la necesidad de contar con un seguro de delincuencia cibernética. Por último, se reconoce la importancia de la privacidad de los empleados en el sector privado y las políticas de privacidad empiezan a ser institucionalizadas.

La sensibilización pública de la seguridad cibernética es generalmente baja y la sociedad toma pocas medidas para protegerse de las amenazas cibernéticas. En respuesta a lo anterior, el ICE y otras fundaciones han liderado campañas de sensibilización, aunque con una difusión limitada y pocos mecanismos de medición. Cada vez hay disponibles más oportunidades para la educación y formación en seguridad cibernética en Costa Rica a través de programas de pregrado, maestría y certificación que ofrece la Universidad Cenfotec.

POBLACIÓN TOTAL DEL PAÍS	**4.757.606**
Abonos a teléfonos celulares	7.101.893
Personas con acceso a Internet	2.331.227

Penetración de Internet

49%



Política y estrategia

Estrategia nacional de seguridad cibernética oficial o documentada

- Desarrollo de la estrategia
- Organización
- Contenido

Defensa cibernética

- Estrategia
- Organización
- Coordinación

Cultura y sociedad

Mentalidad de seguridad cibernética

- En el gobierno
- En el sector privado
- En la sociedad

Conciencia de seguridad cibernética

- Sensibilización

Confianza en el uso de Internet

- En los servicios en línea
- En el gobierno electrónico
- En el comercio electrónico

Privacidad en línea

- Normas de privacidad
- Privacidad del empleado

Educación

Disponibilidad nacional de la educación y formación cibernéticas

- Educación
- Formación

Desarrollo nacional de la educación de seguridad cibernética

- Desarrollo nacional de la educación de seguridad cibernética

Formación e iniciativas educativas públicas y privadas

- Capacitación de empleados en seguridad cibernética

Gobernanza corporativa, conocimiento y normas

- Comprensión de la seguridad cibernética por parte de empresas privadas y estatales

Marcos legales

Marcos jurídicos de seguridad cibernética

- Para la seguridad de las TIC
- Privacidad, protección de datos y otros derechos humanos
- Derecho sustantivo de delincuencia cibernética
- Derecho procesal de delincuencia cibernética

Investigación jurídica

- Cumplimiento de la ley
- La fiscalía
- Tribunales

Divulgación responsable de la información

- Divulgación responsable de la información

Tecnologías

Adhesión a las normas

- Aplicación de las normas y prácticas mínimas aceptables
- Adquisiciones
- Desarrollo de softwre

Organizaciones de coordinación de seguridad cibernética

- Centro de mando y control
- Capacidad de respuesta a incidentes

Respuesta a incidentes

- Identificación y designación
- Organización
- Coordinación

Resiliencia de la infraestructura nacional

- Infraestructura tecnológica
- Resiliencia nacional

Protección de la Infraestructura Crítica Nacional (ICN)

- Identificación
- Organización
- Planeación de respuesta
- Coordinación
- Gestión de riesgos

Gestión de crisis

- Planeación
- Evaluación

Redundancia digital

- Planeación
- Organización

Mercado de la ciberseguridad

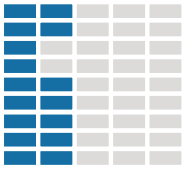
- Tecnologías de seguridad cibernética
- Seguros de delincuencia cibernética

.dm

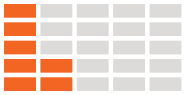
Dominica (Commonwealth de)

Política y estrategia

Cultura y sociedad

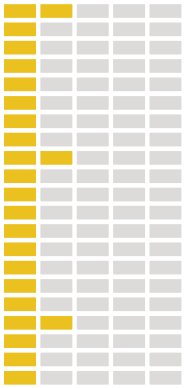


Educación



Marcos legales

Tecnología



Aunque ha comenzado con muy poca infraestructura existente, el Gobierno del Commonwealth de Dominica ha dado grandes pasos en los últimos años para desarrollar una política y estrategia nacional de seguridad cibernética. En coordinación con la OEA, la Iniciativa de Delincuencia Cibernética del Commonwealth (CCI, por sus siglas en inglés) y el Consejo de Europa (CoE, por sus siglas en inglés), Dominica ha diseñado una propuesta de Estrategia Nacional de Seguridad Cibernética. Además de describir los riesgos nacionales y las metas de desarrollo, la propuesta de estrategia define los mandatos para la creación de un CSIRT nacional.

La principal autoridad de lucha contra el delito cibernético, el Departamento de Investigaciones Criminales de la Fuerza Policial del Commonwealth de Dominica, es la única entidad encargada de controlar e investigar los casos de delincuencia cibernética en el país. A pesar de la falta de un laboratorio forense digital, ha logrado un éxito considerable. Actualmente el gobierno del país está elaborando una ley integral de crimen cibernético para ser adoptada en el Parlamento, y busca la adhesión a la Convención del Consejo de Europa sobre la Delincuencia Cibernética (comúnmente conocida como la "Convención de Budapest"), un tratado internacional. Sin embargo no existe, en gran medida, una legislación sobre privacidad y protección de datos.

Aunque su proyecto de estrategia describe riesgos nacionales importantes, Dominica no tiene una política de defensa cibernética coordinada. En casos de eventos cibernéticos, las funciones de mando y control se manejan ad hoc por departamentos del gobierno. Mientras que los dueños de la infraestructura crítica entienden los riesgos de seguridad cibernética y la tecnología de la Infraestructura Crítica Nacional en general cumple con las normas internacionales de la Unión Internacional de Telecomunicaciones, la resiliencia nacional y las gestiones de respuesta se llevan a cabo de manera informal, sin ninguna estructura global.

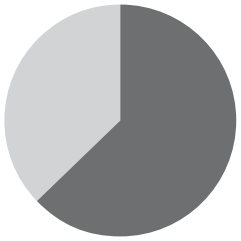
Empresas líderes, como instituciones financieras, y algunos servicios de comercio electrónico han tomado medidas proactivas para aumentar la sensibilización del sector privado ante el phishing y otros ataques cibernéticos, y están comenzando a institucionalizar los estándares de privacidad para los empleados. Sin embargo, la sociedad civil generalmente desconoce las amenazas cibernéticas. Como parte de su proyecto de estrategia, el Gobierno de Dominica está desarrollando campañas de sensibilización para abordar este problema.

El Centro de Capacitación de Negocios del Dominica State College y un puñado de instituciones académicas en línea y privadas ofrecen educación y formación relacionada con la seguridad cibernética, pero sin la coordinación o aportes del Ministerio de Educación, o el establecimiento de alianzas público-privadas. No obstante el Gobierno de Dominica ha organizado una serie de conferencias regionales e internacionales para compartir las mejores prácticas en materia de seguridad cibernética.

POBLACIÓN TOTAL DEL PAÍS	**72.341**
Abonos a teléfonos celulares	92.200
Personas con acceso a Internet	45.575

Penetración de Internet

63%



Política y estrategia

Estrategia nacional de seguridad cibernética oficial o documentada

- Desarrollo de la estrategia
- Organización
- Contenido

Defensa cibernética

- Estrategia
- Organización
- Coordinación

Cultura y sociedad

Mentalidad de seguridad cibernética

- En el gobierno
- En el sector privado
- En la sociedad

Conciencia de seguridad cibernética

- Sensibilización

Confianza en el uso de Internet

- En los servicios en línea
- En el gobierno electrónico
- En el comercio electrónico

Privacidad en línea

- Normas de privacidad
- Privacidad del empleado

Educación

Disponibilidad nacional de la educación y formación cibernéticas

- Educación
- Formación

Desarrollo nacional de la educación de seguridad cibernética

- Desarrollo nacional de la educación de seguridad cibernética

Formación e iniciativas educativas públicas y privadas

- Capacitación de empleados en seguridad cibernética

Gobernanza corporativa, conocimiento y normas

- Comprensión de la seguridad cibernética por parte de empresas privadas y estatales

Marcos legales

Marcos jurídicos de seguridad cibernética

- Para la seguridad de las TIC
- Privacidad, protección de datos y otros derechos humanos
- Derecho sustantivo de delincuencia cibernética
- Derecho procesal de delincuencia cibernética

Investigación jurídica

- Cumplimiento de la ley
- La fiscalía
- Tribunales

Divulgación responsable de la información

- Divulgación responsable de la información

Tecnologías

Adhesión a las normas

- Aplicación de las normas y prácticas mínimas aceptables
- Adquisiciones
- Desarrollo de softwre

Organizaciones de coordinación de seguridad cibernética

- Centro de mando y control
- Capacidad de respuesta a incidentes

Respuesta a incidentes

- Identificación y designación
- Organización
- Coordinación

Resiliencia de la infraestructura nacional

- Infraestructura tecnológica
- Resiliencia nacional

Protección de la Infraestructura Crítica Nacional (ICN)

- Identificación
- Organización
- Planeación de respuesta
- Coordinación
- Gestión de riesgos

Gestión de crisis

- Planeación
- Evaluación

Redundancia digital

- Planeación
- Organización

Mercado de la ciberseguridad

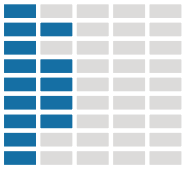
- Tecnologías de seguridad cibernética
- Seguros de delincuencia cibernética

.ec

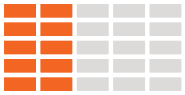
Ecuador

Política y estrategia

Cultura y sociedad

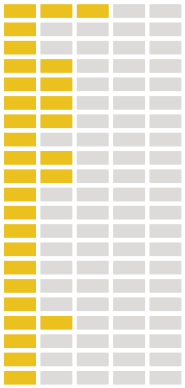


Educación



Marcos legales

Tecnología



A pesar de que no ha desarrollado una estrategia nacional de seguridad cibernética, Ecuador ha hecho avances en los últimos años para fortalecer su capacidad para abordar las amenazas informáticas. Ha designado a la Dirección de Arquitectura Tecnológica y Seguridad de la Información para la promoción de una plataforma de gobierno electrónico y la coordinación de la gestión de la seguridad cibernética. El Centro de Operaciones Tecnológicas Estratégicas y Contrainteligencia de la Secretaría de Inteligencia se encarga de los aspectos técnicos de la seguridad cibernética del país y un CSIRT nacional, el EcuCERT, entró en funcionamiento en noviembre de 2013. A finales de 2013 las entidades pusieron a prueba su temple cuando fueron alertados de una amenaza de un "hackaton", dirigida a la Secretaría de Inteligencia que afortunadamente no se materializó. Las fuerzas militares no han articulado una política de defensa cibernética nacional, pero están trabajando en la asignación de los líderes para un programa. Sin embargo, el país ha instituido medidas para proteger la infraestructura gubernamental de los ataques cibernéticos, incluido el Decreto 166 que requiere que toda la tecnología de la Administración Pública Central cumpla con las normas de seguridad.

La Ley n° 2002-67 proporciona el marco general de los delitos informáticos y el gobierno busca el apoyo de múltiples partes interesadas para instituir reformas al Código Orgánico Integral Penal para abordar de manera más adecuada la delincuencia cibernética. El gobierno está cerca de convertir en ley la protección de datos. La Constitución del Ecuador establece las libertades de expresión y de prensa. Sin embargo, el nuevo Código Penal ha sido criticado por tener el potencial de limitar la libertad de expresión de los ciudadanos[13].

La Unidad de Investigación del Cibercrimen de la Dirección Nacional de la Policía Judicial e Investigaciones se encarga de investigar los delitos cibernéticos. Esta coopera con INTERPOL y ha estado trabajando en el logro de una mayor cooperación interinstitucional, fomentando el intercambio de información con el sector privado y la elaboración de un programa de capacitación en evidencia digital para la policía, los detectives y los tribunales.

La falta de conciencia en la sociedad plantea uno de los mayores desafíos a la seguridad cibernética en el país. Los ataques cibernéticos se incrementaron significativamente en los últimos años pero la mayoría de los afectados no conocían los medios más eficaces para la denuncia de estos incidentes. Para solucionar este problema, la Secretaría de Inteligencia ha liderado la campaña "Promoción de una cultura de inteligencia". Si bien las oportunidades de educación en seguridad cibernética son limitadas, la academia y el sector privado han presentado propuestas para el desarrollo de software y cursos de seguridad cibernética.

POBLACIÓN TOTAL DEL PAÍS	**15.902.916**
Abonos a teléfonos celulares	16.605.737
Personas con acceso a Internet	6.838.254

Penetración de Internet

43%

Política y estrategia

Estrategia nacional de seguridad cibernética oficial o documentada

- Desarrollo de la estrategia
- Organización
- Contenido

Defensa cibernética

- Estrategia
- Organización
- Coordinación

Cultura y sociedad

Mentalidad de seguridad cibernética

- En el gobierno
- En el sector privado
- En la sociedad

Conciencia de seguridad cibernética

- Sensibilización

Confianza en el uso de Internet

- En los servicios en línea
- En el gobierno electrónico
- En el comercio electrónico

Privacidad en línea

- Normas de privacidad
- Privacidad del empleado

Educación

Disponibilidad nacional de la educación y formación cibernéticas

- Educación
- Formación

Desarrollo nacional de la educación de seguridad cibernética

- Desarrollo nacional de la educación de seguridad cibernética

Formación e iniciativas educativas públicas y privadas

- Capacitación de empleados en seguridad cibernética

Gobernanza corporativa, conocimiento y normas

- Comprensión de la seguridad cibernética por parte de empresas privadas y estatales

Marcos legales

Marcos jurídicos de seguridad cibernética

- Para la seguridad de las TIC
- Privacidad, protección de datos y otros derechos humanos
- Derecho sustantivo de delincuencia cibernética
- Derecho procesal de delincuencia cibernética

Investigación jurídica

- Cumplimiento de la ley
- La fiscalía
- Tribunales

Divulgación responsable de la información

- Divulgación responsable de la información

Tecnologías

Adhesión a las normas

- Aplicación de las normas y prácticas mínimas aceptables
- Adquisiciones
- Desarrollo de softwre

Organizaciones de coordinación de seguridad cibernética

- Centro de mando y control
- Capacidad de respuesta a incidentes

Respuesta a incidentes

- Identificación y designación
- Organización
- Coordinación

Resiliencia de la infraestructura nacional

- Infraestructura tecnológica
- Resiliencia nacional

Protección de la Infraestructura Crítica Nacional (ICN)

- Identificación
- Organización
- Planeación de respuesta
- Coordinación
- Gestión de riesgos

Gestión de crisis

- Planeación
- Evaluación

Redundancia digital

- Planeación
- Organización

Mercado de la ciberseguridad

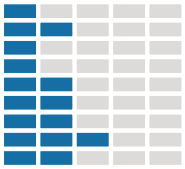
- Tecnologías de seguridad cibernética
- Seguros de delincuencia cibernética

.sv

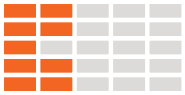
El Salvador

Política y estrategia

Cultura y sociedad

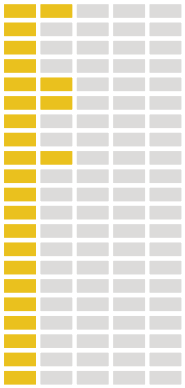


Educación



Marcos legales

Tecnología



El Ministerio de Justicia y Seguridad Pública de El Salvador es el principal organismo nacional encargado de la seguridad cibernética. Actualmente desarrolla una estrategia nacional de seguridad cibernética pero aún no ha divulgado la propuesta completa. También trabaja para asegurar que los datos del gobierno están respaldados y que se practican los estándares de seguridad en todas las infraestructuras de TI. El país tiene un CSIRT nacional, el SalCERT, que responde a los ataques cibernéticos y coordina con otros equipos de respuesta regionales. El SalCERT ha tenido cierto éxito en el seguimiento y la lucha contra amenazas, pero su capacidad es limitada debido a restricciones presupuestales.

Aunque las Fuerzas Armadas de El Salvador han identificado riesgos y áreas importantes de infraestructura a ser protegidas, no existe una política oficial de defensa cibernética. Sin embargo el gobierno maneja formalmente la seguridad de la Infraestructura Crítica Nacional y está planeando ejercicios de gestión de riesgos para establecer las funciones y responsabilidades e identificar las brechas en la seguridad cibernética.

La Asamblea Legislativa de El Salvador ha promulgado leyes sobre protección de datos y acceso a la información pública que establecen normas para la transparencia y la libertad de información así como para la protección de la información personal de los ciudadanos. También ha elaborado proyectos de ley sobre delincuencia cibernética que están en espera de adopción. Existe un mecanismo formal para la solicitud de divulgación por parte del sector privado en casos de delitos cibernéticos; sin embargo las solicitudes deben ser emitidas directamente desde la Fiscalía General de la República, lo que puede retrasar las gestiones de investigación. La División de Ciberdelito de la Policía Nacional Civil investiga los delitos cibernéticos en el país y se ha asociado con la Oficina de las Naciones Unidas contra la Droga y el Delito (ONUDD) para llevar a cabo ejercicios de construcción de capacidad. Dado que la División de Ciberdelito no tiene un laboratorio forense digital, recibe apoyo técnico del SalCERT y ha investigado con éxito varios casos, entre ellos uno en el que atrapó a un depredador sexual involucrado en captación infantil con fines sexuales (grooming).

Con una tasa de penetración de Internet del 30%, la mayor parte de la sociedad salvadoreña generalmente no es consciente de la seguridad cibernética[14]. Hasta la fecha no ha habido campañas de sensibilización en el país. Por otra parte, las universidades actualmente no tienen la capacidad de oferta de oportunidades de educación en seguridad cibernética pero el gobierno está tratando de construir este tipo de programas. Por otro lado, el sector privado ha desarrollado una fuerte mentalidad en seguridad cibernética y reconoce la necesidad de tener seguridad por parte de los servicios de comercio electrónico y ofrece capacitación en seguridad cibernética a los empleados.

POBLACIÓN TOTAL DEL PAÍS	**6.107.706**
Abonos a teléfonos celulares	9.194.242
Personas con acceso a Internet	1.832.312

Penetración de Internet

30%

Política y estrategia

Estrategia nacional de seguridad cibernética oficial o documentada

- Desarrollo de la estrategia
- Organización
- Contenido

Defensa cibernética

- Estrategia
- Organización
- Coordinación

Cultura y sociedad

Mentalidad de seguridad cibernética

- En el gobierno
- En el sector privado
- En la sociedad

Conciencia de seguridad cibernética

- Sensibilización

Confianza en el uso de Internet

- En los servicios en línea
- En el gobierno electrónico
- En el comercio electrónico

Privacidad en línea

- Normas de privacidad
- Privacidad del empleado

Educación

Disponibilidad nacional de la educación y formación cibernéticas

- Educación
- Formación

Desarrollo nacional de la educación de seguridad cibernética

- Desarrollo nacional de la educación de seguridad cibernética

Formación e iniciativas educativas públicas y privadas

- Capacitación de empleados en seguridad cibernética

Gobernanza corporativa, conocimiento y normas

- Comprensión de la seguridad cibernética por parte de empresas privadas y estatales

Marcos legales

Marcos jurídicos de seguridad cibernética

- Para la seguridad de las TIC
- Privacidad, protección de datos y otros derechos humanos
- Derecho sustantivo de delincuencia cibernética
- Derecho procesal de delincuencia cibernética

Investigación jurídica

- Cumplimiento de la ley
- La fiscalía
- Tribunales

Divulgación responsable de la información

- Divulgación responsable de la información

Tecnologías

Adhesión a las normas

- Aplicación de las normas y prácticas mínimas aceptables
- Adquisiciones
- Desarrollo de softwre

Organizaciones de coordinación de seguridad cibernética

- Centro de mando y control
- Capacidad de respuesta a incidentes

Respuesta a incidentes

- Identificación y designación
- Organización
- Coordinación

Resiliencia de la infraestructura nacional

- Infraestructura tecnológica
- Resiliencia nacional

Protección de la Infraestructura Crítica Nacional (ICN)

- Identificación
- Organización
- Planeación de respuesta
- Coordinación
- Gestión de riesgos

Gestión de crisis

- Planeación
- Evaluación

Redundancia digital

- Planeación
- Organización

Mercado de la ciberseguridad

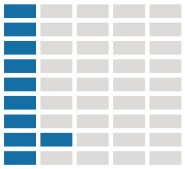
- Tecnologías de seguridad cibernética
- Seguros de delincuencia cibernética

.gd

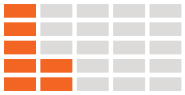
Granada

Política y estrategia

Cultura y sociedad

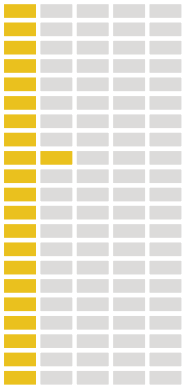


Educación



Marcos legales

Tecnología



En 2012 una asociación entre el Gobierno de Granada y la Unión Internacional de Telecomunicaciones evaluó el estado de preparación en materia de seguridad cibernética del país e hizo recomendaciones para el desarrollo de políticas más firmes[15]. Desde 2012 Granada ha expresado la necesidad de tener un CSIRT nacional. La Comisión Nacional Reguladora de Telecomunicaciones (NTRC, por sus siglas en Inglés) se encarga de desarrollar la estrategia y la política de seguridad cibernética; sin embargo a 2015 no se han formado ni una estrategia nacional ni un CSIRT. La Comisión Nacional Reguladora de Telecomunicaciones también ayuda a coordinar la seguridad para los operadores de la Infraestructura Crítica Nacional, pero las autoridades han informado que en la actualidad desempeña un rol limitado. Mientras que el gobierno en general no está capacitado en seguridad cibernética, la Policía Real de Granada, la principal entidad del país para la defensa cibernética y la investigación de delincuencia cibernética, ha recibido capacitación en seguridad cibernética del Programa de Asistencia Antiterrorista del Gobierno de Estados Unidos.

La división de las TIC de la Policía Real de Granada investiga las violaciones a la seguridad cibernética y los delitos cibernéticos. Un miembro de la fuerza informó que desde 2012 hasta 2015 se investigaron 21 casos. De aquellos que llegaron a la corte, uno fue procesado con éxito y uno estaba en progreso. Sin embargo, la ausencia de un mecanismo de divulgación formal para el sector privado puede obstaculizar las gestiones para descubrir la delincuencia cibernética. Aunque la Policía Real de Granada cuenta con algunos equipos para el análisis forense digital, existe la necesidad de contar con actualizaciones de software y otras herramientas. Por otra parte, el Poder Judicial por lo general carece de la capacidad de corte digital necesaria para manejar evidencia electrónica.

En 2013 el Parlamento de Granada aprobó la Ley de Delitos Electrónicos, que agregó formalmente el delito cibernético al Código Penal y estableció procedimientos para su fiscalización. Como algunas disposiciones de la ley alentaron un escrutinio sobre su potencial para limitar las libertades civiles, el Parlamento decidió modificar dichas secciones con el fin de proteger la libertad de expresión. A pesar de que aún no ha sido adoptada, Granada también ha elaborado una legislación para la protección de datos y la libertad de información.

A medida que la conectividad a Internet se expande en Granada, se han puesto a disposición muchos nuevos servicios de comercio electrónico. Las juntas de directivos de las empresas privadas tienen una cierta comprensión de la seguridad cibernética y están considerando la implementación de mayores estándares de seguridad para las normas de tecnología y privacidad de los empleados. Aunque la tecnología de las infraestructuras críticas nacionales pueden seguir las normas aplicadas por los desarrolladores iniciales, su funcionamiento a menudo se realiza bajo un control gubernamental limitado. Actualmente en el país no hay programas de grado en seguridad cibernética u otras oportunidades educativas relacionadas para los ciudadanos granadinos.

POBLACIÓN TOTAL DEL PAÍS	**106.349**
Abonos a teléfonos celulares	134.500
Personas con acceso a Internet	39.349

Penetración de Internet

37%

Política y estrategia

Estrategia nacional de seguridad cibernética oficial o documentada

- Desarrollo de la estrategia
- Organización
- Contenido

Defensa cibernética

- Estrategia
- Organización
- Coordinación

Cultura y sociedad

Mentalidad de seguridad cibernética

- En el gobierno
- En el sector privado
- En la sociedad

Conciencia de seguridad cibernética

- Sensibilización

Confianza en el uso de Internet

- En los servicios en línea
- En el gobierno electrónico
- En el comercio electrónico

Privacidad en línea

- Normas de privacidad
- Privacidad del empleado

Educación

Disponibilidad nacional de la educación y formación cibernéticas

- Educación
- Formación

Desarrollo nacional de la educación de seguridad cibernética

- Desarrollo nacional de la educación de seguridad cibernética

Formación e iniciativas educativas públicas y privadas

- Capacitación de empleados en seguridad cibernética

Gobernanza corporativa, conocimiento y normas

- Comprensión de la seguridad cibernética por parte de empresas privadas y estatales

Marcos legales

Marcos jurídicos de seguridad cibernética

- Para la seguridad de las TIC
- Privacidad, protección de datos y otros derechos humanos
- Derecho sustantivo de delincuencia cibernética
- Derecho procesal de delincuencia cibernética

Investigación jurídica

- Cumplimiento de la ley
- La fiscalía
- Tribunales

Divulgación responsable de la información

- Divulgación responsable de la información

Tecnologías

Adhesión a las normas

- Aplicación de las normas y prácticas mínimas aceptables
- Adquisiciones
- Desarrollo de softwre

Organizaciones de coordinación de seguridad cibernética

- Centro de mando y control
- Capacidad de respuesta a incidentes

Respuesta a incidentes

- Identificación y designación
- Organización
- Coordinación

Resiliencia de la infraestructura nacional

- Infraestructura tecnológica
- Resiliencia nacional

Protección de la Infraestructura Crítica Nacional (ICN)

- Identificación
- Organización
- Planeación de respuesta
- Coordinación
- Gestión de riesgos

Gestión de crisis

- Planeación
- Evaluación

Redundancia digital

- Planeación
- Organización

Mercado de la ciberseguridad

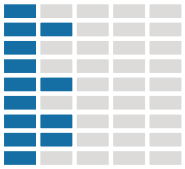
- Tecnologías de seguridad cibernética
- Seguros de delincuencia cibernética

.gt

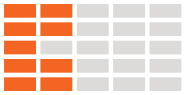
Guatemala

Política y estrategia

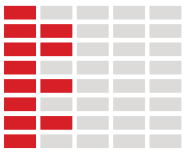
Cultura y sociedad



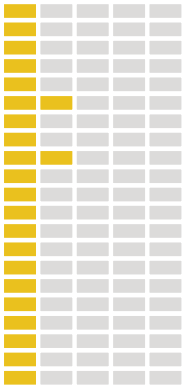
Educación



Marcos legales



Tecnología



Aunque entidades gubernamentales líderes han comenzado a darle prioridad a los asuntos de seguridad cibernética y evaluar los riesgos nacionales, Guatemala no tiene una estrategia nacional de seguridad cibernética expresa. Su principal entidad de seguridad cibernética es el Equipo de Respuesta a Incidentes de Seguridad Informática nacional, el CSIRT-gt, un equipo ad hoc que históricamente ha operado bajo el Ministerio de Defensa. El CSIRT-gt ha recibido capacitación de la OEA y otras instituciones internacionales. Recientemente, el Ministerio de Gobernación también ha mostrado interés en ir avanzando en los temas de seguridad cibernética en Guatemala.

Con la asistencia ofrecida por el CSIRT-gt, las fuerzas del orden tienen una cierta capacidad para investigar ataques y delincuencia cibernéticas, pero las autoridades manifiestan que hasta que no se cuente con una legislación integral sobre delincuencia cibernética, el sistema judicial tendrá dificultades para procesar los casos eficazmente. Por otra parte, no existe una política de divulgación y aparte de ciertas instituciones financieras, el sector privado rara vez informa al gobierno de eventos cibernéticos. Sin embargo el sector privado tiene su propia entidad de respuesta a incidentes, el CERT Cyberseg.

A raíz de un aumento en ataques cibernéticos contra la infraestructura del gobierno en los últimos años, las entidades guatemaltecas han comenzado a tomar medidas para proteger sus activos nacionales, aunque con poca comunicación formal[16]. Los operadores de la Infraestructura Crítica Nacional han desplegado algunas medidas de seguridad y software que cumplen con la norma ISO 27000 y otras normas internacionales. La infraestructura de tecnología suele tercerizarse y el gobierno tiene un control mínimo de la misma.

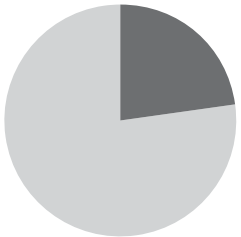
Teniendo en cuenta que la tasa de penetración de Internet en el país es del 23% y que su población es en gran parte rural, es inconsistente la asimilación de una mentalidad de seguridad cibernética en la sociedad[17]. Al mismo tiempo, el gobierno electrónico y los servicios de comercio electrónico en Guatemala han crecido considerablemente en los últimos años. Los miembros del Congreso han trabajado para abordar este tema mediante la formación del Frente Parlamentario de las Tecnologías de la Información y la Comunicación, que además de promover la legislación contra la delincuencia cibernética, tiene como objetivo promover la conciencia de seguridad cibernética y mejorar las normas y mejores prácticas en el sector privado y la sociedad civil.

Aunque Guatemala no cuenta con una estrategia a nivel nacional para el desarrollo de la educación de seguridad cibernética, una universidad técnica y varias empresas privadas ofrecen títulos y certificaciones en seguridad de la información. Además hay una serie de profesionales con certificación CISSP ("Certified Information Systems Security Professional" en inglés). Los próximos pasos incluyen la implementación de un programa de capacitación conjunto público-privado para los empleados del gobierno y del sector privado, que será administrado por el CSIRT-gt en asociación con un proveedor de servicios.

POBLACIÓN TOTAL DEL PAÍS	**16.015.494**
Abonos a teléfonos celulares	16.911.811
Personas con acceso a Internet	3.683.564

Penetración de Internet

23%



Política y estrategia

Estrategia nacional de seguridad cibernética oficial o documentada

- Desarrollo de la estrategia
- Organización
- Contenido

Defensa cibernética

- Estrategia
- Organización
- Coordinación

Cultura y sociedad

Mentalidad de seguridad cibernética

- En el gobierno
- En el sector privado
- En la sociedad

Conciencia de seguridad cibernética

- Sensibilización

Confianza en el uso de Internet

- En los servicios en línea
- En el gobierno electrónico
- En el comercio electrónico

Privacidad en línea

- Normas de privacidad
- Privacidad del empleado

Educación

Disponibilidad nacional de la educación y formación cibernéticas

- Educación
- Formación

Desarrollo nacional de la educación de seguridad cibernética

- Desarrollo nacional de la educación de seguridad cibernética

Formación e iniciativas educativas públicas y privadas

- Capacitación de empleados en seguridad cibernética

Gobernanza corporativa, conocimiento y normas

- Comprensión de la seguridad cibernética por parte de empresas privadas y estatales

Marcos legales

Marcos jurídicos de seguridad cibernética

- Para la seguridad de las TIC
- Privacidad, protección de datos y otros derechos humanos
- Derecho sustantivo de delincuencia cibernética
- Derecho procesal de delincuencia cibernética

Investigación jurídica

- Cumplimiento de la ley
- La fiscalía
- Tribunales

Divulgación responsable de la información

- Divulgación responsable de la información

Tecnologías

Adhesión a las normas

- Aplicación de las normas y prácticas mínimas aceptables
- Adquisiciones
- Desarrollo de softwre

Organizaciones de coordinación de seguridad cibernética

- Centro de mando y control
- Capacidad de respuesta a incidentes

Respuesta a incidentes

- Identificación y designación
- Organización
- Coordinación

Resiliencia de la infraestructura nacional

- Infraestructura tecnológica
- Resiliencia nacional

Protección de la Infraestructura Crítica Nacional (ICN)

- Identificación
- Organización
- Planeación de respuesta
- Coordinación
- Gestión de riesgos

Gestión de crisis

- Planeación
- Evaluación

Redundancia digital

- Planeación
- Organización

Mercado de la ciberseguridad

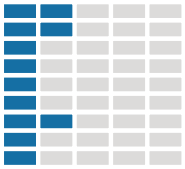
- Tecnologías de seguridad cibernética
- Seguros de delincuencia cibernética

.gy

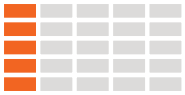
Guyana

Política y estrategia

Cultura y sociedad

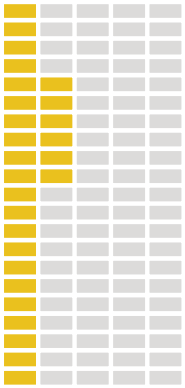


Educación



Marcos legales

Tecnología



Desde el año 2013, Guyana y el resto de la región del Caribe han visto un aumento en los ataques cibernéticos[18]. En agosto de ese año el Gobierno de Guyana estableció su Equipo de Respuesta a Incidentes de Seguridad Informática nacional, el CSIRT.GY, ubicado bajo el Ministerio del Interior. Como mecanismo principal de respuesta a los incidentes relacionados con la seguridad cibernética del país, el CSIRT-GY presta la colaboración en el lugar, la coordinación de incidentes, análisis de incidentes, el soporte técnico, documentación y consejos sobre la seguridad cibernética. También coordina regularmente con la OEA y otros CSIRT nacionales para fortalecer la capacidad técnica y compartir mejores prácticas e información y está comenzando a establecer líneas de comunicación con el sector privado. Sin embargo, el alcance del CSIRT-GY es limitado por la ausencia de una estrategia de seguridad cibernética nacional o política de defensa cibernética y la falta de conciencia sobre los asuntos de seguridad cibernética en el gobierno. Por otra parte, los propietarios de la Infraestructura Crítica Nacional no siempre cumplen con los estándares de seguridad o denuncian los incidentes, y el Estado no ha evaluado formalmente los activos y vulnerabilidades de la ICN.

Cuando se produce un delito cibernético, el Departamento de Investigación Criminal de la Policía de Guyana es responsable de investigar el caso. Aunque las investigaciones se han llevado a cabo con cierto éxito, los fiscales y el Poder Judicial están inadecuadamente capacitados para manejar evidencia electrónica. Los vacíos legislativos son un obstáculo adicional: Guyana cuenta con algún derecho procesal para manejar la evidencia electrónica, pero carece de una ley sustantiva de delito cibernético o legislación relacionada con la el mal uso del sistema de red de computadoras, privacidad y la protección de datos.

A medida que crecen las oportunidades de banca en línea y otros servicios de comercio electrónico, las entidades del sector privado de Guyana comienzan a darle prioridad a la seguridad cibernética como algo importante. En consecuencia, las partes interesadas han comenzado a invertir en la formación de seguridad cibernética para sus empleados, y no solo para aquellos con funciones de TI. Actualmente el gobierno tiene una lista de profesionales ad hoc certificados en seguridad cibernética.

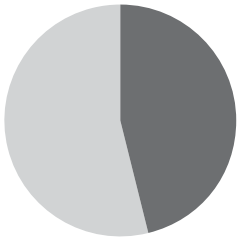
Por otro lado, en la sociedad civil la conciencia de seguridad cibernética es generalmente baja. Aunque el CSIRT-GY ha explorado la posibilidad de realizar una campaña de sensibilización, hasta la fecha ni esta ni ninguna otra entidad han liderado una. Por último, la educación superior ofrece títulos en ciencias informáticas; sin embargo la estrategia nacional de educación de Guyana no incluye temas de seguridad cibernética en sus planes de estudio.

Recientemente el gobierno mostró su compromiso para avanzar en la agenda de la seguridad cibernética organizando un taller nacional sobre las amenazas y las tendencias de seguridad cibernética, el desarrollo de una estrategia nacional de seguridad cibernética y capacitación técnica sobre herramientas de respuesta a incidentes[19].

POBLACIÓN TOTAL DEL PAÍS	**763.893**
Abonos a teléfonos celulares	566.905
Personas con acceso a Internet	282.640

Penetración de Internet

37%



Política y estrategia

Estrategia nacional de seguridad cibernética oficial o documentada

- Desarrollo de la estrategia
- Organización
- Contenido

Defensa cibernética

- Estrategia
- Organización
- Coordinación

Cultura y sociedad

Mentalidad de seguridad cibernética

- En el gobierno
- En el sector privado
- En la sociedad

Conciencia de seguridad cibernética

- Sensibilización

Confianza en el uso de Internet

- En los servicios en línea
- En el gobierno electrónico
- En el comercio electrónico

Privacidad en línea

- Normas de privacidad
- Privacidad del empleado

Educación

Disponibilidad nacional de la educación y formación cibernéticas

- Educación
- Formación

Desarrollo nacional de la educación de seguridad cibernética

- Desarrollo nacional de la educación de seguridad cibernética

Formación e iniciativas educativas públicas y privadas

- Capacitación de empleados en seguridad cibernética

Gobernanza corporativa, conocimiento y normas

- Comprensión de la seguridad cibernética por parte de empresas privadas y estatales

Marcos legales

Marcos jurídicos de seguridad cibernética

- Para la seguridad de las TIC
- Privacidad, protección de datos y otros derechos humanos
- Derecho sustantivo de delincuencia cibernética
- Derecho procesal de delincuencia cibernética

Investigación jurídica

- Cumplimiento de la ley
- La fiscalía
- Tribunales

Divulgación responsable de la información

- Divulgación responsable de la información

Tecnologías

Adhesión a las normas

- Aplicación de las normas y prácticas mínimas aceptables
- Adquisiciones
- Desarrollo de softwre

Organizaciones de coordinación de seguridad cibernética

- Centro de mando y control
- Capacidad de respuesta a incidentes

Respuesta a incidentes

- Identificación y designación
- Organización
- Coordinación

Resiliencia de la infraestructura nacional

- Infraestructura tecnológica
- Resiliencia nacional

Protección de la Infraestructura Crítica Nacional (ICN)

- Identificación
- Organización
- Planeación de respuesta
- Coordinación
- Gestión de riesgos

Gestión de crisis

- Planeación
- Evaluación

Redundancia digital

- Planeación
- Organización

Mercado de la ciberseguridad

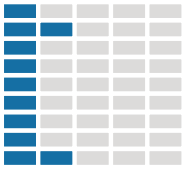
- Tecnologías de seguridad cibernética
- Seguros de delincuencia cibernética

.ht

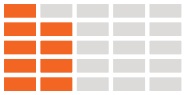
Haití

Política y estrategia

Cultura y sociedad

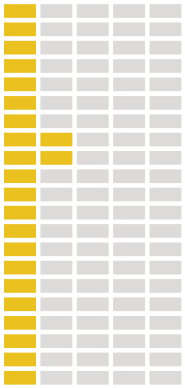


Educación



Marcos legales

Tecnología



Aunque se encuentran con recursos limitados y ha habido algunos reveses en los últimos años, las entidades del Gobierno de Haití continúan trabajando hacia la elaboración de una estrategia nacional de seguridad cibernética y el desarrollo de un CSIRT nacional. Un grupo de trabajo conformado por la unidad de gobierno electrónico del Gabinete del Primer Ministro (PRIMATURE), el Consejo Nacional de Telecomunicaciones (CONATEL), la Policía Nacional y la Secretaría para la Seguridad Nacional se ha reunido para establecer el marco para una estrategia nacional y han recibido asistencia de la OEA, la Unión Internacional de Telecomunicaciones y otros socios internacionales. Recientemente se estableció un grupo de trabajo dentro del CONATEL con el mandato de elaborar un plan estratégico y un plan de trabajo para la seguridad cibernética y la lucha contra el delito cibernético.

Si bien el conocimiento sobre la seguridad cibernética en el gobierno es cada vez mayor, la preparación varía según las agencias. Esto es notorio en la falta de aplicación uniforme de las normas de seguridad a través de las infraestructuras de TI. Sin embargo la principal preocupación del CONATEL ha sido la necesidad de tener una capacidad de respuesta a incidentes cibernéticos y se ha coordinado con el sector privado para abogar por la creación de un CSIRT.

Como parte del Proyecto HIPCAR de la Unión de Telecomunicaciones del Caribe (CTU) y la Comunidad del Caribe (CARICOM), las partes interesadas haitianas han propuesto legislación sobre la delincuencia cibernética y leyes de privacidad de Internet que se encuentran actualmente en la fase de consulta. Sin embargo, las gestiones legislativas se han estancado dado el desacuerdo sobre las elecciones que llevó a la disolución de la mayoría del Parlamento de Haití en enero de 2015[20]. Hasta que se resuelva esta crisis política, será muy difícil que el país adopte un marco jurídico integral para la delincuencia cibernética. No obstante, la Dirección Central de la Policía Judicial (DCPJ) ha tenido un éxito considerable en la investigación y detención de la delincuencia cibernética por medio de la captura de 69 delincuentes en 2014, de los cuales 11 fueron declarados culpables de delitos relacionados con la cibernética.

Con una tasa de penetración de Internet del 11%, la conciencia de seguridad cibernética en la sociedad haitiana es predominantemente baja[21]. Para solucionar esto, el CONATEL ha llevado a cabo una serie de eventos para brindar conocimientos a las partes interesadas y al público en general sobre la seguridad cibernética. Así mismo algunas universidades ofrecen cursos relacionados con la seguridad cibernética, pero actualmente no hay programas de grado formales. Áreas del sector privado, como los bancos y los operadores de telecomunicaciones, están bien informados de la importancia de la seguridad cibernética y han invertido en oportunidades de formación para los empleados. Mientras que los servicios de gobierno electrónico están empezando a llegar al país recién ahora, los servicios de comercio electrónico están ampliamente disponibles y por lo general son confiables y seguros.

POBLACIÓN TOTAL DEL PAÍS	**10.572.029**
Abonos a teléfonos celulares	6.769.312
Personas con acceso a Internet	1.162.923

Penetración de Internet

11%

Política y estrategia

Estrategia nacional de seguridad cibernética oficial o documentada

- Desarrollo de la estrategia
- Organización
- Contenido

Defensa cibernética

- Estrategia
- Organización
- Coordinación

Cultura y sociedad

Mentalidad de seguridad cibernética

- En el gobierno
- En el sector privado
- En la sociedad

Conciencia de seguridad cibernética

- Sensibilización

Confianza en el uso de Internet

- En los servicios en línea
- En el gobierno electrónico
- En el comercio electrónico

Privacidad en línea

- Normas de privacidad
- Privacidad del empleado

Educación

Disponibilidad nacional de la educación y formación cibernéticas

- Educación
- Formación

Desarrollo nacional de la educación de seguridad cibernética

- Desarrollo nacional de la educación de seguridad cibernética

Formación e iniciativas educativas públicas y privadas

- Capacitación de empleados en seguridad cibernética

Gobernanza corporativa, conocimiento y normas

- Comprensión de la seguridad cibernética por parte de empresas privadas y estatales

Marcos legales

Marcos jurídicos de seguridad cibernética

- Para la seguridad de las TIC
- Privacidad, protección de datos y otros derechos humanos
- Derecho sustantivo de delincuencia cibernética
- Derecho procesal de delincuencia cibernética

Investigación jurídica

- Cumplimiento de la ley
- La fiscalía
- Tribunales

Divulgación responsable de la información

- Divulgación responsable de la información

Tecnologías

Adhesión a las normas

- Aplicación de las normas y prácticas mínimas aceptables
- Adquisiciones
- Desarrollo de softwre

Organizaciones de coordinación de seguridad cibernética

- Centro de mando y control
- Capacidad de respuesta a incidentes

Respuesta a incidentes

- Identificación y designación
- Organización
- Coordinación

Resiliencia de la infraestructura nacional

- Infraestructura tecnológica
- Resiliencia nacional

Protección de la Infraestructura Crítica Nacional (ICN)

- Identificación
- Organización
- Planeación de respuesta
- Coordinación
- Gestión de riesgos

Gestión de crisis

- Planeación
- Evaluación

Redundancia digital

- Planeación
- Organización

Mercado de la ciberseguridad

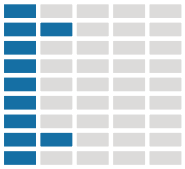
- Tecnologías de seguridad cibernética
- Seguros de delincuencia cibernética

.hn

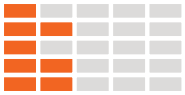
Honduras

Política y estrategia

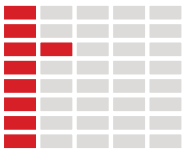
Cultura y sociedad



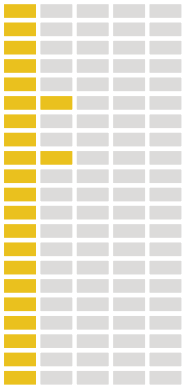
Educación



Marcos legales



Tecnología



A falta de una política nacional de seguridad cibernética o un equipo de respuesta a incidentes, el Gobierno de Honduras tiene una capacidad limitada para abordar de manera proactiva las amenazas a su seguridad cibernética. Como conoce estos riesgos, el gobierno ha adoptado una serie de medidas, entre ellas: trabajar para renovar su estrategia de seguridad nacional para incluir los temas de seguridad y delincuencia cibernética; asistir a foros internacionales ofrecidos por la OEA y otras instituciones en cuestiones de planificación de gestión de crisis; e incorporar programas digitales en organismos como la Comisión Nacional de Telecomunicaciones (CONATEL) y la Dirección Presidencial de Gestión por Resultados a cargo de la "Agenda Digital" del Estado. Así mismo, las partes interesadas de la Infraestructura Crítica Nacional están implementando tecnologías de seguridad y normas internacionales, incluyendo ISACA, ISO 27002 e ITIL ("Information Technology Infrastructure Library" en inglés), para proteger mejor los activos nacionales. Sin embargo la gestión de tecnologías de seguridad es descoordinada y a menudo se subcontrata con terceros y no existe una política en marcha para la divulgación de las violaciones a la seguridad.

Honduras carece de un marco legislativo para la seguridad de las TIC; su legislatura está actualmente llevando a cabo reformas al código penal que introducirían leyes contra la delincuencia cibernética. La Dirección Nacional de Información Criminal de la Policía Nacional es la única entidad del país responsable de investigar los delitos cibernéticos, pero carece de un laboratorio forense digital o estadísticas nacionales sobre delincuencia cibernética.

El Gobierno de Honduras ha promulgado una legislación parcial respecto a la privacidad, la protección de datos y la protección de la libertad de expresión. Con un bajo nivel de penetración de Internet (18%) y altos niveles de violencia relacionada con pandillas, la sociedad en general desconfía de los servicios en línea proporcionados por el gobierno y en su mayoría desconoce las amenazas cibernéticas[22].

El sector privado proporciona un contraejemplo en términos de mentalidad en seguridad cibernética. Con el apoyo del gobierno, algunas organizaciones privadas del sector financiero en Honduras han establecido políticas de alto nivel y pautas de seguridad cibernética para sus organizaciones. Estos documentos proporcionan una política de seguridad cibernética en general para los empleados dentro de estas organizaciones. Sin embargo aún no se han implementado, de manera efectiva, medidas para proteger la privacidad de los empleados. Por último, aunque la formación en materia de seguridad cibernética no está muy extendida a nivel nacional, muchas empresas internacionales de TI y algunas universidades ofrecen cursos y capacitación en seguridad cibernética para los estudiantes y empleados hondureños.

POBLACIÓN TOTAL DEL PAÍS	**7.961.680**
Abonos a teléfonos celulares	7.725.092
Personas con acceso a Internet	1.512.719

Penetración de Internet

19%

Política y estrategia

Estrategia nacional de seguridad cibernética oficial o documentada

- Desarrollo de la estrategia
- Organización
- Contenido

Defensa cibernética

- Estrategia
- Organización
- Coordinación

Cultura y sociedad

Mentalidad de seguridad cibernética

- En el gobierno
- En el sector privado
- En la sociedad

Conciencia de seguridad cibernética

- Sensibilización

Confianza en el uso de Internet

- En los servicios en línea
- En el gobierno electrónico
- En el comercio electrónico

Privacidad en línea

- Normas de privacidad
- Privacidad del empleado

Educación

Disponibilidad nacional de la educación y formación cibernéticas

- Educación
- Formación

Desarrollo nacional de la educación de seguridad cibernética

- Desarrollo nacional de la educación de seguridad cibernética

Formación e iniciativas educativas públicas y privadas

- Capacitación de empleados en seguridad cibernética

Gobernanza corporativa, conocimiento y normas

- Comprensión de la seguridad cibernética por parte de empresas privadas y estatales

Marcos legales

Marcos jurídicos de seguridad cibernética

- Para la seguridad de las TIC
- Privacidad, protección de datos y otros derechos humanos
- Derecho sustantivo de delincuencia cibernética
- Derecho procesal de delincuencia cibernética

Investigación jurídica

- Cumplimiento de la ley
- La fiscalía
- Tribunales

Divulgación responsable de la información

- Divulgación responsable de la información

Tecnologías

Adhesión a las normas

- Aplicación de las normas y prácticas mínimas aceptables
- Adquisiciones
- Desarrollo de softwre

Organizaciones de coordinación de seguridad cibernética

- Centro de mando y control
- Capacidad de respuesta a incidentes

Respuesta a incidentes

- Identificación y designación
- Organización
- Coordinación

Resiliencia de la infraestructura nacional

- Infraestructura tecnológica
- Resiliencia nacional

Protección de la Infraestructura Crítica Nacional (ICN)

- Identificación
- Organización
- Planeación de respuesta
- Coordinación
- Gestión de riesgos

Gestión de crisis

- Planeación
- Evaluación

Redundancia digital

- Planeación
- Organización

Mercado de la ciberseguridad

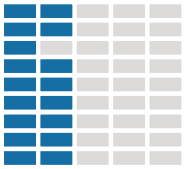
- Tecnologías de seguridad cibernética
- Seguros de delincuencia cibernética

.jm

Jamaica

Política y estrategia

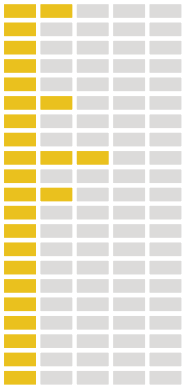
Cultura y sociedad



Educación

Marcos legales

Tecnología



En 2013 el Gobierno de Jamaica no tenía en marcha ni una política ni una estrategia de seguridad cibernética. Dos años después, ya ha diseñado una estrategia nacional integral, presentada el 28 de enero de 2015, y se encuentra creando un CSIRT nacional. A la cabeza de estos desarrollos está el Grupo Nacional de Trabajo de Seguridad Cibernética, establecido bajo el Ministerio de Ciencia, Tecnología, Energía y Minería. El Programa de Seguridad Cibernética de la OEA y otras organizaciones internacionales han ayudado a Jamaica en el desarrollo de su CSIRT. Cabe destacar que a raíz de una serie de ataques cibernéticos contra sitios web del gobierno a finales de 2014, la OEA envió un equipo de expertos a Kingston para dar apoyo en la gestión de incidentes[23]. Las autoridades de defensa cibernética han recibido capacitación después de este incidente, pero a diferencia del gobierno civil, no cuentan con una política unificada. Los próximos grandes retos en seguridad cibernética para el Gobierno de Jamaica serán asegurar la adhesión generalizada a los estándares y coordinar la seguridad de la Infraestructura Crítica Nacional, ya que los operadores tienen cierta capacidad para proteger sus infraestructuras críticas frente a las amenazas, pero la seguridad no es gestionada formalmente por el gobierno.

En marzo de 2010 Jamaica aprobó la Ley de Delitos Cibernéticos. En 2013 el Parlamento, en correspondencia con los cambios en la tecnología y las amenazas, organizó una comisión para informar sobre el estado de la legislación y hacer revisiones según era necesario. La Unidad de Comunicación Forense y Delito Cibernético del Cuerpo de Policía de Jamaica es un organismo completamente funcional en la aplicación de la ley, designado para investigar los delitos cibernéticos. La Unidad de Comunicación Forense y Delito Cibernético tiene su propio laboratorio de análisis forense digital. Uno de los retos al que se enfrentan las fuerzas del orden público es el subregistro de incidentes por parte de las partes afectadas; por lo tanto el Ministerio de Ciencia, Tecnología, Energía y Minería ha estado presionando a la legislatura para que entre en vigencia una ley de divulgación responsable. Por último, aunque Jamaica cuenta con una legislación específica de delincuencia cibernética, solo existe una legislación parcial para la protección de datos y privacidad.

Empresas del sector privado han comenzado a gestionar los riesgos de seguridad cibernética y poner en práctica políticas de privacidad para los empleados, pero la conciencia de la importancia de la seguridad cibernética varía considerablemente en la sociedad en general. Para hacer frente a este tipo de vacíos en el conocimiento, el Grupo Nacional de Trabajo de Seguridad Cibernética tiene un Memorando de Entendimiento con el programa STOP.THINK.CONNECT. de la Alianza Nacional de Seguridad Cibernética, una campaña internacional dirigida a educar al público acerca de la seguridad en Internet. Además la Estrategia Nacional de Seguridad Cibernética de Jamaica incluye un mandato para incorporar la seguridad cibernética en los programas de educación que actualmente se encuentra en sus etapas preliminares.

POBLACIÓN TOTAL DEL PAÍS	**2.721.252**
Abonos a teléfonos celulares	2.880.589
Personas con acceso a Internet	1.115.713

Penetración de Internet

41%

Política y estrategia

Estrategia nacional de seguridad cibernética oficial o documentada

- Desarrollo de la estrategia
- Organización
- Contenido

Defensa cibernética

- Estrategia
- Organización
- Coordinación

Cultura y sociedad

Mentalidad de seguridad cibernética

- En el gobierno
- En el sector privado
- En la sociedad

Conciencia de seguridad cibernética

- Sensibilización

Confianza en el uso de Internet

- En los servicios en línea
- En el gobierno electrónico
- En el comercio electrónico

Privacidad en línea

- Normas de privacidad
- Privacidad del empleado

Educación

Disponibilidad nacional de la educación y formación cibernéticas

- Educación
- Formación

Desarrollo nacional de la educación de seguridad cibernética

- Desarrollo nacional de la educación de seguridad cibernética

Formación e iniciativas educativas públicas y privadas

- Capacitación de empleados en seguridad cibernética

Gobernanza corporativa, conocimiento y normas

- Comprensión de la seguridad cibernética por parte de empresas privadas y estatales

Marcos legales

Marcos jurídicos de seguridad cibernética

- Para la seguridad de las TIC
- Privacidad, protección de datos y otros derechos humanos
- Derecho sustantivo de delincuencia cibernética
- Derecho procesal de delincuencia cibernética

Investigación jurídica

- Cumplimiento de la ley
- La fiscalía
- Tribunales

Divulgación responsable de la información

- Divulgación responsable de la información

Tecnologías

Adhesión a las normas

- Aplicación de las normas y prácticas mínimas aceptables
- Adquisiciones
- Desarrollo de softwre

Organizaciones de coordinación de seguridad cibernética

- Centro de mando y control
- Capacidad de respuesta a incidentes

Respuesta a incidentes

- Identificación y designación
- Organización
- Coordinación

Resiliencia de la infraestructura nacional

- Infraestructura tecnológica
- Resiliencia nacional

Protección de la Infraestructura Crítica Nacional (ICN)

- Identificación
- Organización
- Planeación de respuesta
- Coordinación
- Gestión de riesgos

Gestión de crisis

- Planeación
- Evaluación

Redundancia digital

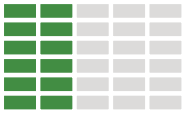
- Planeación
- Organización

Mercado de la ciberseguridad

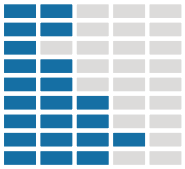
- Tecnologías de seguridad cibernética
- Seguros de delincuencia cibernética

México

Política y estrategia



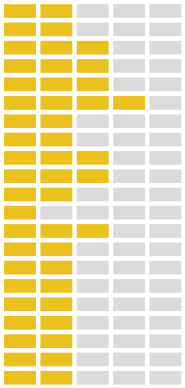
Cultura y sociedad



Educación

Marcos legales

Tecnología



El Gobierno de México trabaja actualmente en la elaboración de una estrategia nacional de seguridad cibernética, desarrollando una política escrita que considera la defensa cibernética a cargo de las Fuerzas Armadas. El Equipo de Respuesta a Incidentes de Seguridad Informática del país, CERT-MX, es un miembro del Foro Mundial de Respuesta a Incidentes y Equipos de Seguridad (FIRST) y sigue un Protocolo de Colaboración con otras entidades gubernamentales. El CERT-MX está muy involucrado en la protección de la Infraestructura Crítica Nacional (ICN). Los interesados coordinan la gestión de seguridad de infraestructuras y comparten información sobre los activos y las vulnerabilidades de la ICN. En todas las agencias gubernamentales, las tecnologías se actualizan regularmente, se realizan copias de seguridad y se adhiere a las disposiciones del Manual Administrativo de Aplicación General de Tecnologías de Información y Comunicaciones y de Seguridad de la Información (MAAGTICSI), el cual se desarrolló con base a normas internacionales como ISO 27001, ITIL ("Information Technology Infrastructure Library" en inglés) y COBIT ("Control Objectives for Information and Related Technology" en inglés), entre otras. Por otra parte, están en marcha planes de redundancia digital.

La División Científica de la Policía Federal de México investiga los delitos cibernéticos nacionales. Trabaja en estrecha colaboración con el CERT-MX y ha recibido capacitación por parte de organizaciones sin ánimo de lucro y de varias organizaciones internacionales. Informes recientes indican un aumento de la suplantación de identidad (phishing) y amenazas persistentes avanzadas en el país y una disminución de los ataques de denegación de servicio DoS (por sus siglas en inglés, Denial of Service). Si bien las fuerzas del orden cuentan con una amplia capacidad de investigación, México aún está desarrollando una legislación integral sobre delincuencia cibernética, lo que dificulta el enjuiciamiento de tales actos.

Con una tasa de penetración de Internet del 44%, se requiere emprender un esfuerzo para informar a la sociedad mexicana sobre los problemas de seguridad cibernética. Instituciones gubernamentales y la academia ofrecen conferencias sobre seguridad cibernética.[24] También están disponibles algunas oportunidades de capacitación para empleados, incluyendo programas de certificación a través del sector privado. Recientemente el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) inició una campaña proponiendo leyes más estrictas de protección de datos personales, así como una mayor transparencia y disponibilidad de información al público. Además de su labor de promoción, el INAI publica informes y conduce campañas de sensibilización para los ciudadanos sobre sus derechos como usuarios de las tecnologías de la información y la comunicación.

POBLACIÓN TOTAL DEL PAÍS	**125.385.833**
Abonos a teléfonos celulares	102.187.895
Personas con acceso a Internet	55.169.767

Penetración de Internet

44%

Política y estrategia

Estrategia nacional de seguridad cibernética oficial o documentada

- Desarrollo de la estrategia
- Organización
- Contenido

Defensa cibernética

- Estrategia
- Organización
- Coordinación

Cultura y sociedad

Mentalidad de seguridad cibernética

- En el gobierno
- En el sector privado
- En la sociedad

Conciencia de seguridad cibernética

- Sensibilización

Confianza en el uso de Internet

- En los servicios en línea
- En el gobierno electrónico
- En el comercio electrónico

Privacidad en línea

- Normas de privacidad
- Privacidad del empleado

Educación

Disponibilidad nacional de la educación y formación cibernéticas

- Educación
- Formación

Desarrollo nacional de la educación de seguridad cibernética

- Desarrollo nacional de la educación de seguridad cibernética

Formación e iniciativas educativas públicas y privadas

- Capacitación de empleados en seguridad cibernética

Gobernanza corporativa, conocimiento y normas

- Comprensión de la seguridad cibernética por parte de empresas privadas y estatales

Marcos legales

Marcos jurídicos de seguridad cibernética

- Para la seguridad de las TIC
- Privacidad, protección de datos y otros derechos humanos
- Derecho sustantivo de delincuencia cibernética
- Derecho procesal de delincuencia cibernética

Investigación jurídica

- Cumplimiento de la ley
- La fiscalía
- Tribunales

Divulgación responsable de la información

- Divulgación responsable de la información

Tecnologías

Adhesión a las normas

- Aplicación de las normas y prácticas mínimas aceptables
- Adquisiciones
- Desarrollo de softwre

Organizaciones de coordinación de seguridad cibernética

- Centro de mando y control
- Capacidad de respuesta a incidentes

Respuesta a incidentes

- Identificación y designación
- Organización
- Coordinación

Resiliencia de la infraestructura nacional

- Infraestructura tecnológica
- Resiliencia nacional

Protección de la Infraestructura Crítica Nacional (ICN)

- Identificación
- Organización
- Planeación de respuesta
- Coordinación
- Gestión de riesgos

Gestión de crisis

- Planeación
- Evaluación

Redundancia digital

- Planeación
- Organización

Mercado de la ciberseguridad

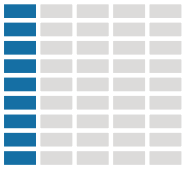
- Tecnologías de seguridad cibernética
- Seguros de delincuencia cibernética

.ni

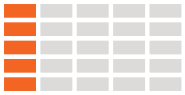
Nicaragua

Política y estrategia

Cultura y sociedad

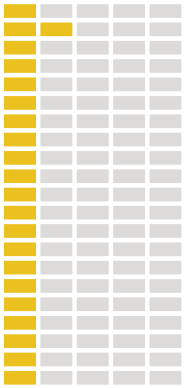


Educación



Marcos legales

Tecnología



El Consejo Nicaragüense de Ciencia y Tecnología (CONICYT) trabaja en el desarrollo de políticas nacionales y el aumento de la conciencia de seguridad cibernética, mientras que la Comisión de Gobierno Electrónico de Nicaragua (GOBeNIC) adelanta programas de gobierno electrónico y facilita la discusión entre el gobierno y las industrias de infraestructura crítica. Hasta la fecha, Nicaragua no ha desarrollado una estrategia o política de seguridad cibernética nacional y el país no tiene un CSIRT formal para responder a incidentes cibernéticos. El CONICYT y la GOBeNIC, por lo tanto, ven como parte indispensable de su misión convencer a legisladores y altos funcionarios del gobierno de invertir mucho más en seguridad cibernética y promulgar políticas, leyes y normas para proteger mejor los intereses nacionales frente a las amenazas cibernéticas.

El Código Penal de Nicaragua contiene cláusulas para judicializar la delincuencia cibernética y en 2012 la Asamblea Nacional sancionó la Ley de Protección de Datos n° 787. Si bien no hay una oficina formal de investigación de delincuencia cibernética, la División de Crímenes Especiales y la Dirección de Inteligencia Policial de la Policía Nacional manejan rutinariamente los casos de evidencia electrónica. La Policía Nacional también cuenta con un Laboratorio Central de Criminalística, que les proporciona análisis forense digital a las otras divisiones. Si bien el personal ocasionalmente colabora con organizaciones regionales e internacionales, cuyo ejemplo notable es el caso en el que INTERPOL y Nicaragua cooperaron con España para revelar toda una red de pedofilia, en general la cooperación internacional sigue siendo limitada.

Aunque el Código Penal exige que cualquier persona comparta información relacionada con un delito en investigación con las autoridades competentes, el sector privado no está legalmente obligado a revelar brechas en la seguridad cibernética. En cambio, los investigadores deben solicitar formalmente información de los proveedores de servicios de Internet pertinentes. Un estudio realizado en 2014 por la empresa de software de antivirus ESET mostró que al menos el 50% de todas las empresas nicaragüenses han sido objeto de un ataque cibernético[25]. Si bien las empresas en general aplican los estándares de seguridad, a menudo no capacitan a los empleados en seguridad cibernética; sin embargo un número de universidades ofrecen cursos y capacitación especializada en el tema.

En mayo de 2015 el CONICYT se asoció con la academia y el sector privado para poner en marcha por primera vez la Semana del Uso Seguro de Internet, una serie de charlas, foros y actividades dedicados a concientizar al público sobre seguridad cibernética y promover mejores prácticas para el uso seguro de las TI[26].

POBLACIÓN TOTAL DEL PAÍS	**5.945.646**
Abonos a teléfonos celulares	7.067.860
Personas con acceso a Internet	1.070.216

Penetración de Internet

18%

Política y estrategia

Estrategia nacional de seguridad cibernética oficial o documentada

- Desarrollo de la estrategia
- Organización
- Contenido

Defensa cibernética

- Estrategia
- Organización
- Coordinación

Cultura y sociedad

Mentalidad de seguridad cibernética

- En el gobierno
- En el sector privado
- En la sociedad

Conciencia de seguridad cibernética

- Sensibilización

Confianza en el uso de Internet

- En los servicios en línea
- En el gobierno electrónico
- En el comercio electrónico

Privacidad en línea

- Normas de privacidad
- Privacidad del empleado

Educación

Disponibilidad nacional de la educación y formación cibernéticas

- Educación
- Formación

Desarrollo nacional de la educación de seguridad cibernética

- Desarrollo nacional de la educación de seguridad cibernética

Formación e iniciativas educativas públicas y privadas

- Capacitación de empleados en seguridad cibernética

Gobernanza corporativa, conocimiento y normas

- Comprensión de la seguridad cibernética por parte de empresas privadas y estatales

Marcos legales

Marcos jurídicos de seguridad cibernética

- Para la seguridad de las TIC
- Privacidad, protección de datos y otros derechos humanos
- Derecho sustantivo de delincuencia cibernética
- Derecho procesal de delincuencia cibernética

Investigación jurídica

- Cumplimiento de la ley
- La fiscalía
- Tribunales

Divulgación responsable de la información

- Divulgación responsable de la información

Tecnologías

Adhesión a las normas

- Aplicación de las normas y prácticas mínimas aceptables
- Adquisiciones
- Desarrollo de softwre

Organizaciones de coordinación de seguridad cibernética

- Centro de mando y control
- Capacidad de respuesta a incidentes

Respuesta a incidentes

- Identificación y designación
- Organización
- Coordinación

Resiliencia de la infraestructura nacional

- Infraestructura tecnológica
- Resiliencia nacional

Protección de la Infraestructura Crítica Nacional (ICN)

- Identificación
- Organización
- Planeación de respuesta
- Coordinación
- Gestión de riesgos

Gestión de crisis

- Planeación
- Evaluación

Redundancia digital

- Planeación
- Organización

Mercado de la ciberseguridad

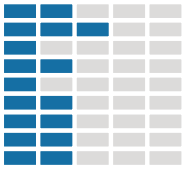
- Tecnologías de seguridad cibernética
- Seguros de delincuencia cibernética

.pa

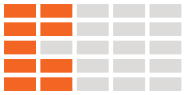
Panamá

Política y estrategia

Cultura y sociedad

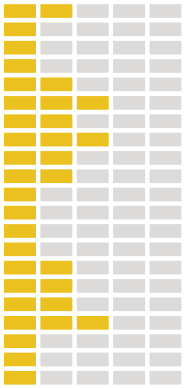


Educación



Marcos legales

Tecnología



Desde mayo de 2013, el Gobierno de Panamá ha estado trabajando en la implementación de su Estrategia Nacional de Seguridad Cibernética y Protección de Infraestructura Crítica (ENSC+IC), desarrollada por la Autoridad Nacional para la Innovación Gubernamental (AIG). Este documento, junto con un informe de posición titulado "La Resiliencia de la Infraestructura Crítica, Protección de Menores en Internet y Seguridad Cibernética", establece metas y diseña papeles y responsabilidades. Desde entonces, las entidades del gobierno han comenzado las etapas iniciales del desarrollo de planes internos de seguridad cibernética. Las publicaciones también intentan abordar la falta de conciencia entre las partes interesadas acerca de la protección de la Infraestructura Crítica Nacional (ICN); y las autoridades han indicado que esta es una de sus principales preocupaciones. A pesar de que se practican algunos estándares de seguridad, en la actualidad existe poca coordinación entre los operadores para la protección de la ICN. El Gobierno ha establecido medidas de redundancia digital. Así mismo, empieza a liderar la formación en gestión de crisis para los equipos de respuesta y los operadores de la ICN. En el caso de un ataque cibernético o evento relacionado, el CSIRT PANAMÁ es el organismo encargado de responder y mitigar el incidente.

Con enmiendas al código penal del país y leyes relativas a la obtención de evidencia, Panamá ha actualizado la legislación nacional para combatir más eficazmente la delincuencia cibernética. A partir de 2009 también han entrado en vigor leyes de protección de datos. En 2014 Panamá adhirió oficialmente al Convenio de Budapest, el primer tratado internacional para abordar la delincuencia cibernética.

Panamá se ocupa de los casos de delincuencia cibernética en dos frentes: a través de la Unidad de Investigaciones de Delitos Informáticos, dependiente de la Dirección de Investigación Judicial, y a través de la Fiscalía Superior Especializada en Delitos contra la Propiedad Intelectual y Seguridad Informática. Las autoridades han indicado un fuerte aumento de los ataques cibernéticos en los últimos años, con 262 casos en 2013. A pesar de que no existe un mecanismo que les exija a las empresas del sector privado reportar perturbaciones a su seguridad cibernética, las autoridades trabajan en estrecha colaboración con bancos, proveedores de energía hidroeléctrica y otros sectores de infraestructura crítica para obtener información sobre ataques cibernéticos.

Una serie de instituciones, incluyendo la Universidad Tecnológica de Panamá, ofrecen títulos avanzados en seguridad cibernética. Están disponibles en el país otras oportunidades de educación y formación. Mientras que muchas se ofrecen sobre una base ad hoc, grupos como el Instituto Tecnológico del Istmo (ITI) ofrecen capacitación regular al personal de infraestructura crítica y los servicios de emergencia. En 2013 Panamá se unió a la campaña internacional STOP.THINK.CONNECT, que tiene como objetivo promover prácticas seguras en Internet.

POBLACIÓN TOTAL DEL PAÍS	**3.867.833**
Abonos a teléfonos celulares	6.205.238
Personas con acceso a Internet	1.740.525

Penetración de Internet

45%

Política y estrategia

Estrategia nacional de seguridad cibernética oficial o documentada

- Desarrollo de la estrategia
- Organización
- Contenido

Defensa cibernética

- Estrategia
- Organización
- Coordinación

Cultura y sociedad

Mentalidad de seguridad cibernética

- En el gobierno
- En el sector privado
- En la sociedad

Conciencia de seguridad cibernética

- Sensibilización

Confianza en el uso de Internet

- En los servicios en línea
- En el gobierno electrónico
- En el comercio electrónico

Privacidad en línea

- Normas de privacidad
- Privacidad del empleado

Educación

Disponibilidad nacional de la educación y formación cibernéticas

- Educación
- Formación

Desarrollo nacional de la educación de seguridad cibernética

- Desarrollo nacional de la educación de seguridad cibernética

Formación e iniciativas educativas públicas y privadas

- Capacitación de empleados en seguridad cibernética

Gobernanza corporativa, conocimiento y normas

- Comprensión de la seguridad cibernética por parte de empresas privadas y estatales

Marcos legales

Marcos jurídicos de seguridad cibernética

- Para la seguridad de las TIC
- Privacidad, protección de datos y otros derechos humanos
- Derecho sustantivo de delincuencia cibernética
- Derecho procesal de delincuencia cibernética

Investigación jurídica

- Cumplimiento de la ley
- La fiscalía
- Tribunales

Divulgación responsable de la información

- Divulgación responsable de la información

Tecnologías

Adhesión a las normas

- Aplicación de las normas y prácticas mínimas aceptables
- Adquisiciones
- Desarrollo de softwre

Organizaciones de coordinación de seguridad cibernética

- Centro de mando y control
- Capacidad de respuesta a incidentes

Respuesta a incidentes

- Identificación y designación
- Organización
- Coordinación

Resiliencia de la infraestructura nacional

- Infraestructura tecnológica
- Resiliencia nacional

Protección de la Infraestructura Crítica Nacional (ICN)

- Identificación
- Organización
- Planeación de respuesta
- Coordinación
- Gestión de riesgos

Gestión de crisis

- Planeación
- Evaluación

Redundancia digital

- Planeación
- Organización

Mercado de la ciberseguridad

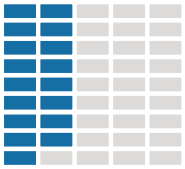
- Tecnologías de seguridad cibernética
- Seguros de delincuencia cibernética

.py

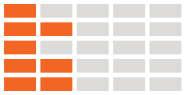
Paraguay

Política y estrategia

Cultura y sociedad

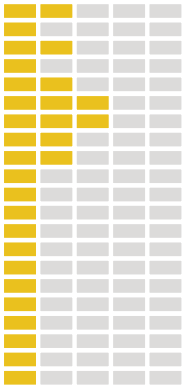


Educación



Marcos legales

Tecnología



La Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICS) de Paraguay está a cargo de la elaboración de las políticas de seguridad cibernética nacionales. El Gobierno de Paraguay no ha adoptado una estrategia nacional de seguridad cibernética pero ha estado trabajando con la OEA desde noviembre de 2014 para desarrollar una. Bajo la operación de la SENATICS, el Equipo de Respuesta de Incidentes de Seguridad Informática de Paraguay, CERT-py, responde a los ataques cibernéticos, mantiene un registro central de los incidentes de seguridad cibernética nacional y promueve la concientización sobre la seguridad cibernética. Ha recibido capacitación de la OEA y del Programa de Asistencia Antiterrorista del Departamento de Estado de EE.UU. Aunque fueron limitados los datos recibidos por parte de los proveedores de servicios de Internet y el sector bancario, en 2014 el CERT-py observó un aumento de ataques de Denegación de Servicio (DoS) y el hacking todavía constituye el mayor porcentaje de ataques.

Los operadores de la Infraestructura Crítica Nacional (ICN) han comenzado a poner en práctica las normas y tecnologías para defender mejor los activos del país contra amenazas cibernéticas. Sin embargo la ICN se gestiona de manera informal y ha habido poca discusión entre las partes interesadas en gestión de riesgos y planificación de respuesta a emergencias.

En los últimos años, el Gobierno del Paraguay ha aprobado leyes para reforzar el marco legislativo y afrontar los delitos cibernéticos. La Ley n° 4439 de 2011 modificó el código penal para incluir tipos de delito cibernético, así como pornografía infantil. Además la Ley n° 1286/98 establece que las entidades están obligadas a reportar los hechos punibles por ley a las autoridades nacionales competentes. Sin embargo su aplicación en delitos relacionados con la seguridad cibernética ha tenido poco éxito. Consecuentemente, el gobierno ha establecido líneas más fuertes de comunicación con el sector bancario. Si bien las leyes relacionadas con la protección de datos y privacidad están en marcha, muchas no son recientes y no abordan explícitamente la información digital. La Unidad Especializada de Delitos Informáticos de la Policía Nacional se encarga de investigar los delitos cibernéticos y cuenta con su propio laboratorio de análisis forense digital.

Las autoridades paraguayas han señalado la falta de conciencia de la sociedad y del sector privado en temas de seguridad cibernética. Para abordar este vacío en el conocimiento, SENATICS lanzó la campaña Conéctate Seguro Paraguay que le informa a la sociedad sobre las amenazas cibernéticas con un enfoque especial en la seguridad de los jóvenes. El Gobierno también se ha asociado con STOP.THINK.CONNECT. Algunas instituciones de educación superior ofrecen cursos en seguridad cibernética, pero actualmente no existen programas de grado en este campo.

POBLACIÓN TOTAL DEL PAÍS	**6.552.518**
Abonos a teléfonos celulares	7.305.277
Personas con acceso a Internet	2.817.583

Penetración de Internet

43%

Política y estrategia

Estrategia nacional de seguridad cibernética oficial o documentada

- Desarrollo de la estrategia
- Organización
- Contenido

Defensa cibernética

- Estrategia
- Organización
- Coordinación

Cultura y sociedad

Mentalidad de seguridad cibernética

- En el gobierno
- En el sector privado
- En la sociedad

Conciencia de seguridad cibernética

- Sensibilización

Confianza en el uso de Internet

- En los servicios en línea
- En el gobierno electrónico
- En el comercio electrónico

Privacidad en línea

- Normas de privacidad
- Privacidad del empleado

Educación

Disponibilidad nacional de la educación y formación cibernéticas

- Educación
- Formación

Desarrollo nacional de la educación de seguridad cibernética

- Desarrollo nacional de la educación de seguridad cibernética

Formación e iniciativas educativas públicas y privadas

- Capacitación de empleados en seguridad cibernética

Gobernanza corporativa, conocimiento y normas

- Comprensión de la seguridad cibernética por parte de empresas privadas y estatales

Marcos legales

Marcos jurídicos de seguridad cibernética

- Para la seguridad de las TIC
- Privacidad, protección de datos y otros derechos humanos
- Derecho sustantivo de delincuencia cibernética
- Derecho procesal de delincuencia cibernética

Investigación jurídica

- Cumplimiento de la ley
- La fiscalía
- Tribunales

Divulgación responsable de la información

- Divulgación responsable de la información

Tecnologías

Adhesión a las normas

- Aplicación de las normas y prácticas mínimas aceptables
- Adquisiciones
- Desarrollo de softwre

Organizaciones de coordinación de seguridad cibernética

- Centro de mando y control
- Capacidad de respuesta a incidentes

Respuesta a incidentes

- Identificación y designación
- Organización
- Coordinación

Resiliencia de la infraestructura nacional

- Infraestructura tecnológica
- Resiliencia nacional

Protección de la Infraestructura Crítica Nacional (ICN)

- Identificación
- Organización
- Planeación de respuesta
- Coordinación
- Gestión de riesgos

Gestión de crisis

- Planeación
- Evaluación

Redundancia digital

- Planeación
- Organización

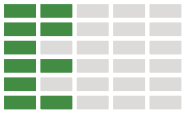
Mercado de la ciberseguridad

- Tecnologías de seguridad cibernética
- Seguros de delincuencia cibernética

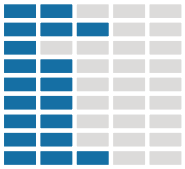
.pe

Perú

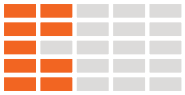
Política y estrategia



Cultura y sociedad

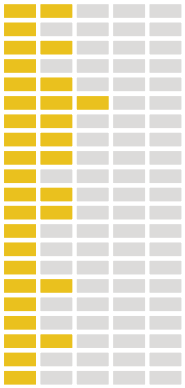


Educación



Marcos legales

Tecnología



Con más de 12 millones de usuarios de Internet (el 40% de la población del país), Perú es un eje regional de actividad y comercio digital y en consecuencia, con riesgos a la seguridad cibernética[27]. Los datos muestran que los incidentes cibernéticos aumentaron un 30% en 2013 y el país experimentó también un incremento de los ataques de malware durante la Copa Mundial de 2014, que se celebró en Brasil. Afortunadamente el Equipo de Respuesta a Incidentes de Seguridad Informática del Perú, PeCERT, respondió con éxito a estos ataques. Además de la respuesta a incidentes, el PeCERT también analiza los asuntos de seguridad con la policía, las fuerzas militares y el sector privado, y está actualizando y ampliando sus capacidades. El Gobierno de Perú ha solicitado la asistencia técnica de la OEA para desarrollar un marco de seguridad cibernética para el país, para lo cual la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI) ha asumido la responsabilidad. Mientras que la conciencia de las partes interesadas ha aumentado con gestiones recientes, la ausencia de una estrategia y una cadena de mando clara continúan impidiendo el fortalecimiento de la seguridad cibernética del país. Las fuerzas armadas también tienen un nivel básico de capacidad de defensa cibernética, pero no existe una política de defensa cibernética.

Tres piezas clave de legislación guían el marco legal para la seguridad cibernética del Perú: la Ley 27309, que incluyó la delincuencia cibernética en el código penal; la Ley 29733 de Protección de Datos; y la Ley 30096, que estableció normas jurídicas relacionadas con la delincuencia cibernética. La División de Investigación de Delitos de Alta Tecnología (DIVINDAT) de la Policía Nacional del Perú (PNP) es la unidad máxima para el manejo de la delincuencia cibernética de esta nación. Equipada con capacidad de laboratorio forense, la DIVINDAT descubrió una serie de recientes ataques cibernéticos dirigidos contra instituciones gubernamentales de alto nivel. Entre los constantes desafíos que se enfrentan, cabe citar su limitada capacidad técnica para el manejo de evidencia electrónica en los tribunales y la falta de una política de divulgación para el sector privado.

El sector privado y los operadores de infraestructura crítica nacional han adoptado algunas normas de seguridad, incluyendo procesos de desarrollo de software. La ONGEI también proporciona directrices sobre la gestión de crisis; sin embargo el alcance de denuncia responsable sigue siendo bajo, ya que las tecnologías de seguridad y la Infraestructura Crítica Nacional (ICN) son gestionadas de manera informal. Las entidades peruanas están discutiendo la posibilidad de contar con un seguro de delincuencia cibernética y otros mecanismos para proteger mejor la ICN.

Mientras que los servicios de gobierno electrónico y comercio electrónico continúan expandiéndose en el Perú, la conciencia social de la seguridad cibernética es generalmente baja. La ONGEI ofrece literatura en línea sobre este tema pero no hay una amplia campaña de sensibilización que esté actualmente vigente. Muchas universidades nacionales y empresas privadas ofrecen educación y capacitación en seguridad cibernética. Sin embargo, suele carecerse de tecnología adecuada y personal educativo con experiencia.

POBLACIÓN TOTAL DEL PAÍS	**30.973.148**
Abonos a teléfonos celulares	31.666.244
Personas con acceso a Internet	12.389.259

Penetración de Internet

40%

Política y estrategia

Estrategia nacional de seguridad cibernética oficial o documentada

- Desarrollo de la estrategia
- Organización
- Contenido

Defensa cibernética

- Estrategia
- Organización
- Coordinación

Cultura y sociedad

Mentalidad de seguridad cibernética

- En el gobierno
- En el sector privado
- En la sociedad

Conciencia de seguridad cibernética

- Sensibilización

Confianza en el uso de Internet

- En los servicios en línea
- En el gobierno electrónico
- En el comercio electrónico

Privacidad en línea

- Normas de privacidad
- Privacidad del empleado

Educación

Disponibilidad nacional de la educación y formación cibernéticas

- Educación
- Formación

Desarrollo nacional de la educación de seguridad cibernética

- Desarrollo nacional de la educación de seguridad cibernética

Formación e iniciativas educativas públicas y privadas

- Capacitación de empleados en seguridad cibernética

Gobernanza corporativa, conocimiento y normas

- Comprensión de la seguridad cibernética por parte de empresas privadas y estatales

Marcos legales

Marcos jurídicos de seguridad cibernética

- Para la seguridad de las TIC
- Privacidad, protección de datos y otros derechos humanos
- Derecho sustantivo de delincuencia cibernética
- Derecho procesal de delincuencia cibernética

Investigación jurídica

- Cumplimiento de la ley
- La fiscalía
- Tribunales

Divulgación responsable de la información

- Divulgación responsable de la información

Tecnologías

Adhesión a las normas

- Aplicación de las normas y prácticas mínimas aceptables
- Adquisiciones
- Desarrollo de softwre

Organizaciones de coordinación de seguridad cibernética

- Centro de mando y control
- Capacidad de respuesta a incidentes

Respuesta a incidentes

- Identificación y designación
- Organización
- Coordinación

Resiliencia de la infraestructura nacional

- Infraestructura tecnológica
- Resiliencia nacional

Protección de la Infraestructura Crítica Nacional (ICN)

- Identificación
- Organización
- Planeación de respuesta
- Coordinación
- Gestión de riesgos

Gestión de crisis

- Planeación
- Evaluación

Redundancia digital

- Planeación
- Organización

Mercado de la ciberseguridad

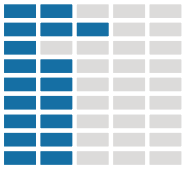
- Tecnologías de seguridad cibernética
- Seguros de delincuencia cibernética

.do

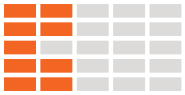
República Dominicana

Política y estrategia

Cultura y sociedad

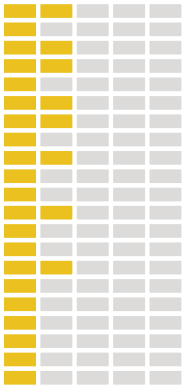


Educación



Marcos legales

Tecnología



Aunque la República Dominicana no tiene ninguna estrategia nacional de seguridad cibernética, ni una política coordinada de defensa cibernética, un número de entidades trabajan conjuntamente para abordar las cuestiones de seguridad cibernética en virtud de la Comisión Interinstitucional contra Crímenes y Delitos de Alta Tecnología (CICDAT). A pesar de la participación de las agencias en la CICDAT, el nivel de sensibilización sobre la seguridad cibernética dentro del gobierno es generalmente bajo. Recién ahora están comenzando los operadores de Infraestructura Crítica Nacional (ICN) a adherirse a los estándares internacionales de tecnologías de información (TI) y a adoptar tecnologías de seguridad. Sin embargo, los operadores de la ICN tienen la capacidad básica de detectar, identificar, proteger, responder y recuperarse de amenazas cibernéticas.

Con la aprobación de la Ley 53-07 y la Ley 310-13, así como la adhesión al Convenio sobre Delincuencia Cibernética (Convenio de Budapest), la República Dominicana ha desarrollado un marco legislativo global para la penalización de la delincuencia cibernética y el manejo de evidencia electrónica, la regulación de correo SPAM y el establecimiento de cooperación internacional. Por otra parte, los tribunales tienen la formación y capacidad suficientes para procesar los casos de evidencia electrónica. Sin embargo, solo existe una legislación parcial en lo que respecta a la privacidad en Internet y la libertad de expresión.

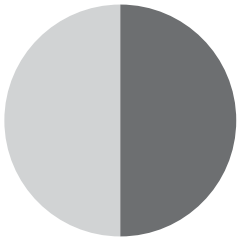
El Departamento de Investigación de Crímenes y Delitos de Alta Tecnología (DICAT) de la Policía Nacional y la División de Investigaciones de Delitos Informáticos (DIDI) del Departamento Nacional de Investigaciones (DNI) son las dos principales entidades de investigación de crímenes cibernéticos en el país. Como la República Dominicana no tiene un CSIRT nacional, el DICAT también maneja la respuesta a incidentes cibernéticos y coordina regularmente con INTERPOL y los CSIRT de otros países. Por último, el gobierno está mejorando la colaboración con el sector privado al divulgar infracciones cibernéticas y proporcionar informes de vulnerabilidad.

Dada la creciente cantidad de usuarios de Internet y disponibilidad de servicios de comercio electrónico, la República Dominicana se enfrenta cada vez más a amenazas cibernéticas. El gobierno del país reportó 963 casos de suplantación de identidad (phishing) en 2013, así como 432 casos de robo de datos bancarios entre 2009 y 2014[28]. A pesar de la iniciativa "Internet Sano" (http://www.Internetsano.do) del Instituto Dominicano de las Telecomunicaciones (INDOTEL), la sensibilización del sector privado sobre seguridad cibernética es moderada y la conciencia social acerca de estos asuntos sigue siendo baja. No obstante, las empresas privadas están reconociendo la privacidad del empleado como un asunto importante y se encuentran adoptando medidas de protección. El gobierno y la academia también están trabajando para crear programas pertinentes, dadas las limitadas oportunidades para educación y formación en seguridad cibernética del país.

POBLACIÓN TOTAL DEL PAÍS	**10.405.943**
Abonos a teléfonos celulares	8.303.536
Personas con acceso a Internet	5.202.972

Penetración de Internet

50%



Política y estrategia

Estrategia nacional de seguridad cibernética oficial o documentada

- Desarrollo de la estrategia
- Organización
- Contenido

Defensa cibernética

- Estrategia
- Organización
- Coordinación

Cultura y sociedad

Mentalidad de seguridad cibernética

- En el gobierno
- En el sector privado
- En la sociedad

Conciencia de seguridad cibernética

- Sensibilización

Confianza en el uso de Internet

- En los servicios en línea
- En el gobierno electrónico
- En el comercio electrónico

Privacidad en línea

- Normas de privacidad
- Privacidad del empleado

Educación

Disponibilidad nacional de la educación y formación cibernéticas

- Educación
- Formación

Desarrollo nacional de la educación de seguridad cibernética

- Desarrollo nacional de la educación de seguridad cibernética

Formación e iniciativas educativas públicas y privadas

- Capacitación de empleados en seguridad cibernética

Gobernanza corporativa, conocimiento y normas

- Comprensión de la seguridad cibernética por parte de empresas privadas y estatales

Marcos legales

Marcos jurídicos de seguridad cibernética

- Para la seguridad de las TIC
- Privacidad, protección de datos y otros derechos humanos
- Derecho sustantivo de delincuencia cibernética
- Derecho procesal de delincuencia cibernética

Investigación jurídica

- Cumplimiento de la ley
- La fiscalía
- Tribunales

Divulgación responsable de la información

- Divulgación responsable de la información

Tecnologías

Adhesión a las normas

- Aplicación de las normas y prácticas mínimas aceptables
- Adquisiciones
- Desarrollo de softwre

Organizaciones de coordinación de seguridad cibernética

- Centro de mando y control
- Capacidad de respuesta a incidentes

Respuesta a incidentes

- Identificación y designación
- Organización
- Coordinación

Resiliencia de la infraestructura nacional

- Infraestructura tecnológica
- Resiliencia nacional

Protección de la Infraestructura Crítica Nacional (ICN)

- Identificación
- Organización
- Planeación de respuesta
- Coordinación
- Gestión de riesgos

Gestión de crisis

- Planeación
- Evaluación

Redundancia digital

- Planeación
- Organización

Mercado de la ciberseguridad

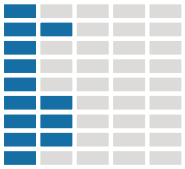
- Tecnologías de seguridad cibernética
- Seguros de delincuencia cibernética

.kn

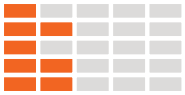
Saint Kitts y Nevis

Política y estrategia

Cultura y sociedad

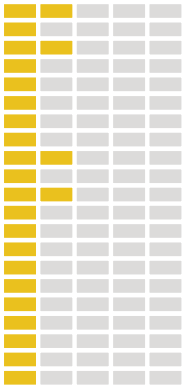


Educación



Marcos legales

Tecnología



Con una penetración de Internet de alrededor del 65%, Saint Kitts y Nevis es uno de los países más conectados del Caribe[29]. Los ciudadanos tienen acceso a un número cada vez mayor de servicios de gobierno electrónico y comercio electrónico. En algunas zonas las capacidades de seguridad cibernética aún no han igualado las necesidades de la creciente comunidad en línea. Saint Kitts y Nevis no cuenta ni con una estrategia nacional de seguridad cibernética ni una política de defensa cibernética. Los asuntos de seguridad cibernética son manejados principalmente por el Ministerio del Empoderamiento de la Juventud, Deportes, Tecnología de Información y Comunicaciones, y Correos, que se ocupa de los asuntos de TIC de manera más general. Las partes interesadas han tomado medidas para proteger la Infraestructura Crítica Nacional (ICN) de las amenazas cibernéticas, lo cual incluye actualizar la tecnología de seguridad, cumplir con las especificaciones de software y mantenerse informado de los activos y las vulnerabilidades de la ICN. Sin embargo el gobierno tiene una capacidad limitada para responder a los incidentes ya que no ha creado un CSIRT. Para solucionar este problema, en marzo de 2015 Saint Kitts y Nevis envió funcionarios a un Curso de Formación de Seguridad Cibernética TRANSITS de la OEA, organizado en colaboración con la Asociación de Redes Transeuropeas de Investigación y Educación (TERENA, por sus siglas en inglés), que se dedica al desarrollo de CSIRT nacionales.

El país no cuenta con una ley o protocolo en marcha que se ocupe específicamente de los delitos cibernéticos, aunque las autoridades informan que el gobierno está discutiendo actualmente la adopción de un marco legal. Sin embargo, ha creado un proyecto de ley de protección de datos y privacidad y recientemente revisó las disposiciones procesales para la obtención de pruebas electrónicas. La Oficina Local de Inteligencia de la Policía Real de Saint Kitts y Nevis, que se coordina con INTERPOL, se ocupa de los casos de delitos cibernéticos, entre otras funciones. Si bien la policía tiene cierta capacidad para investigar los delitos cibernéticos, debe externalizar el análisis forense digital. La falta de una política de divulgación para las empresas del sector privado complica aún más la investigación de los delitos cibernéticos.

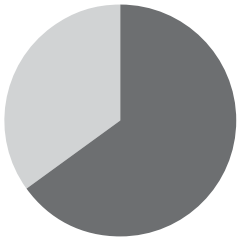
Dadas las abundantes oportunidades de comercio electrónico del país, la administración del sector privado es cada vez más consciente de las amenazas a la seguridad cibernética y ha iniciado una planificación de gestión de riesgos. Por ejemplo, empresas como la multinacional LIME, un proveedor de servicios de comunicaciones, les exige a sus empleados someterse a capacitación en seguridad cibernética.

Con el fin de aumentar la conciencia de seguridad cibernética en el Caribe, Saint Kitts y Nevis organizó una reunión regional público-privada en septiembre de 2014[30]. Sin embargo las oportunidades locales para la educación o formación en seguridad cibernética son limitadas.

POBLACIÓN TOTAL DEL PAÍS	**54.944**
Abonos a teléfonos celulares	76.600
Personas con acceso a Internet	35.714

Penetración de Internet

65%



Política y estrategia

Estrategia nacional de seguridad cibernética oficial o documentada

- Desarrollo de la estrategia
- Organización
- Contenido

Defensa cibernética

- Estrategia
- Organización
- Coordinación

Cultura y sociedad

Mentalidad de seguridad cibernética

- En el gobierno
- En el sector privado
- En la sociedad

Conciencia de seguridad cibernética

- Sensibilización

Confianza en el uso de Internet

- En los servicios en línea
- En el gobierno electrónico
- En el comercio electrónico

Privacidad en línea

- Normas de privacidad
- Privacidad del empleado

Educación

Disponibilidad nacional de la educación y formación cibernéticas

- Educación
- Formación

Desarrollo nacional de la educación de seguridad cibernética

- Desarrollo nacional de la educación de seguridad cibernética

Formación e iniciativas educativas públicas y privadas

- Capacitación de empleados en seguridad cibernética

Gobernanza corporativa, conocimiento y normas

- Comprensión de la seguridad cibernética por parte de empresas privadas y estatales

Marcos legales

Marcos jurídicos de seguridad cibernética

- Para la seguridad de las TIC
- Privacidad, protección de datos y otros derechos humanos
- Derecho sustantivo de delincuencia cibernética
- Derecho procesal de delincuencia cibernética

Investigación jurídica

- Cumplimiento de la ley
- La fiscalía
- Tribunales

Divulgación responsable de la información

- Divulgación responsable de la información

Tecnologías

Adhesión a las normas

- Aplicación de las normas y prácticas mínimas aceptables
- Adquisiciones
- Desarrollo de softwre

Organizaciones de coordinación de seguridad cibernética

- Centro de mando y control
- Capacidad de respuesta a incidentes

Respuesta a incidentes

- Identificación y designación
- Organización
- Coordinación

Resiliencia de la infraestructura nacional

- Infraestructura tecnológica
- Resiliencia nacional

Protección de la Infraestructura Crítica Nacional (ICN)

- Identificación
- Organización
- Planeación de respuesta
- Coordinación
- Gestión de riesgos

Gestión de crisis

- Planeación
- Evaluación

Redundancia digital

- Planeación
- Organización

Mercado de la ciberseguridad

- Tecnologías de seguridad cibernética
- Seguros de delincuencia cibernética

.vc

San Vicente y las Granadinas

Política y estrategia

Cultura y sociedad

Educación

Marcos legales

Tecnología

Si bien la principal entidad responsable de la seguridad cibernética en San Vicente y las Granadinas es la Unidad de Tecnología de Información de la Policía Real de San Vicente y las Granadinas, la Oficina del Primer Ministro también desempeña un papel informal como facilitador de los debates nacionales que rodean la estrategia y la política de seguridad cibernética. En la actualidad, hay una estrategia nacional en la fase de planificación y un CSIRT nacional que se encuentra en desarrollo. Una vez que se hayan completado estos objetivos, San Vicente y las Granadinas habrá aumentado su capacidad para planificar medidas de seguridad cibernética proactivas y no solo reactivas. Si bien la información sobre protección de infraestructuras críticas se limitó en este estudio, un avance reciente notable ha sido la asociación del país con otros Estados de la región del Caribe para adoptar un Sistema Automatizado de Identificación de Huellas Dactilares compartido.

El 4 de mayo de 2015, el sitio web oficial del Gobierno de San Vicente y las Granadinas fue atacado por un hacker que se autoidentificó como parte del Estado Islámico (IS). La Unidad de Tecnología de Información de la Policía Real de San Vicente y las Granadinas tiene la responsabilidad de responder e investigar los ataques cibernéticos y los delitos cibernéticos. La unidad recibe asistencia técnica del Gobierno de los Estados Unidos y participa en capacitaciones regionales organizadas por la OEA, la Unión de Telecomunicaciones del Caribe, INTERPOL y otras organizaciones regionales e internacionales. La unidad no cuenta con un laboratorio forense digital y envía pruebas a Antigua y Barbuda para su análisis; sin embargo recientemente adquirió equipos para desarrollar la capacidad de laboratorio en el país. Aunque las empresas no están obligadas a reportar las violaciones a la seguridad cibernética, la Unidad de Tecnología de Información colabora con el sector privado para investigar los incidentes cibernéticos.

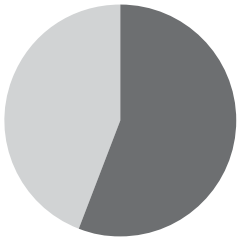
Dos leyes sustentan un marco legislativo básico para la seguridad cibernética en el país: la Ley de Pruebas Electrónicas (2004) y la Ley de Transacciones Electrónicas (2007); sin embargo las autoridades creen que estas leyes requieren actualización y fortalecimiento para combatir eficazmente a la delincuencia cibernética.

La penetración de Internet en San Vicente y las Granadinas ha crecido notablemente en los últimos años, de 38,5% de la población en 2010 a 56% en 2014[31]. Por otra parte el gobierno ha emprendido una ambiciosa iniciativa llamada "Un Computador Portátil Por Estudiante"[32]. Esta expansión en el acceso a la web sin duda ha generado una mayor participación e inclusión en Internet, pero también se ha correspondido con el aumento de incidentes que se producen en las redes sociales de las escuelas. Si bien el gobierno ha reconocido esta creciente preocupación, aún no se ha desarrollado una campaña o programa de sensibilización para hacerle frente.

POBLACIÓN TOTAL DEL PAÍS	**109.360**
Abonos a teléfonos celulares	115.017
Personas con acceso a Internet	61.242

Penetración de Internet

56%



Política y estrategia

Estrategia nacional de seguridad cibernética oficial o documentada

- Desarrollo de la estrategia
- Organización
- Contenido

Defensa cibernética

- Estrategia
- Organización
- Coordinación

Cultura y sociedad

Mentalidad de seguridad cibernética

- En el gobierno
- En el sector privado
- En la sociedad

Conciencia de seguridad cibernética

- Sensibilización

Confianza en el uso de Internet

- En los servicios en línea
- En el gobierno electrónico
- En el comercio electrónico

Privacidad en línea

- Normas de privacidad
- Privacidad del empleado

Educación

Disponibilidad nacional de la educación y formación cibernéticas

- Educación
- Formación

Desarrollo nacional de la educación de seguridad cibernética

- Desarrollo nacional de la educación de seguridad cibernética

Formación e iniciativas educativas públicas y privadas

- Capacitación de empleados en seguridad cibernética

Gobernanza corporativa, conocimiento y normas

- Comprensión de la seguridad cibernética por parte de empresas privadas y estatales

Marcos legales

Marcos jurídicos de seguridad cibernética

- Para la seguridad de las TIC
- Privacidad, protección de datos y otros derechos humanos
- Derecho sustantivo de delincuencia cibernética
- Derecho procesal de delincuencia cibernética

Investigación jurídica

- Cumplimiento de la ley
- La fiscalía
- Tribunales

Divulgación responsable de la información

- Divulgación responsable de la información

Tecnologías

Adhesión a las normas

- Aplicación de las normas y prácticas mínimas aceptables
- Adquisiciones
- Desarrollo de softwre

Organizaciones de coordinación de seguridad cibernética

- Centro de mando y control
- Capacidad de respuesta a incidentes

Respuesta a incidentes

- Identificación y designación
- Organización
- Coordinación

Resiliencia de la infraestructura nacional

- Infraestructura tecnológica
- Resiliencia nacional

Protección de la Infraestructura Crítica Nacional (ICN)

- Identificación
- Organización
- Planeación de respuesta
- Coordinación
- Gestión de riesgos

Gestión de crisis

- Planeación
- Evaluación

Redundancia digital

- Planeación
- Organización

Mercado de la ciberseguridad

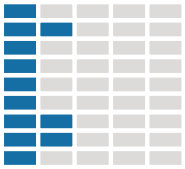
- Tecnologías de seguridad cibernética
- Seguros de delincuencia cibernética

.lc

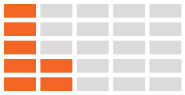
Santa Lucía

Política y estrategia

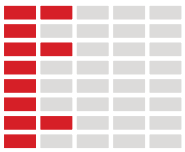
Cultura y sociedad



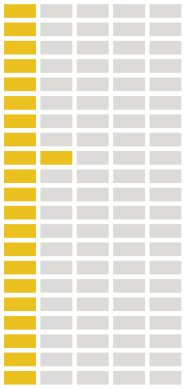
Educación



Marcos legales



Tecnología



En respuesta a un ataque cibernético por un hacker que se identificó como del Estado islámico contra las vecinas San Vicente y las Granadinas en la primavera de 2015, el Gobierno de Santa Lucía anunció sus planes para fortalecer la seguridad cibernética de su país a través de un enfoque multifacético, incluidas normas de seguridad más estrictas para la Infraestructura Crítica Nacional (ICN) y una mayor capacidad para detectar y mitigar las amenazas cibernéticas[33]. La iniciativa está liderada por la Dirección de Modernización del Sector Público del Ministerio de la Función Pública, que supervisa la innovación de la infraestructura de tecnología del gobierno, la expansión de los servicios de gobierno electrónico y los asuntos de seguridad cibernética. Santa Lucía también es miembro de la Alianza Internacional Multilateral contra las Amenazas Cibernéticas de la Unión Internacional de las Telecomunicaciones (ITU-IMPACT, por sus siglas en inglés). Teniendo en cuenta estos recientes pasos, el país no ha desarrollado una estrategia o política de seguridad cibernética nacional formal, y no tiene un CSIRT nacional.

El artículo 267 del Código Penal (2003) de Santa Lucía legisla sobre el fraude informático y delitos cibernéticos relacionados y el artículo 330 tipifica como delito la venta y producción de pornografía infantil. Santa Lucía también ha promulgado ley procesal en la búsqueda e incautación de pruebas electrónicas. El país ha ratificado a la Convención sobre los Derechos del Niño, así como al Protocolo Facultativo de la Convención sobre los Derechos del Niño relativo a la venta de niños, la prostitución infantil y la pornografía infantil, que dispone procesos más detallados sobre la lucha contra el delito.

Los casos de delitos cibernéticos son asunto de la Policía Real de Santa Lucía. Esta recibe el apoyo de la Asociación de Banqueros de Santa Lucía, que la dotó de nuevos equipos para construir su capacidad de investigación de la delincuencia cibernética[34]. Las empresas del sector privado no están obligadas por ley a reportar violaciones en seguridad cibernética a las autoridades, sin embargo no hay ninguna página web establecida o línea telefónica para denunciar los casos relacionados con la protección de la infancia en línea.

Hasta la fecha el gobierno de Santa Lucía no ha liderado una campaña nacional de concientización en materia de seguridad cibernética para la sociedad en general, y las oportunidades de capacitación en seguridad cibernética en el país son limitadas. Sin embargo Santa Lucía contribuyó recientemente a la seguridad cibernética a nivel regional al acoger el Octavo Foro del Caribe de Gobernanza de Internet y el Taller de Seguridad Cibernética, celebrado del 29 al 30 agosto de 2014[35].

POBLACIÓN TOTAL DEL PAÍS	**183.645**
Abonos a teléfonos celulares	188.351
Personas con acceso a Internet	93.659

Penetración de Internet

51%

Política y estrategia

Estrategia nacional de seguridad cibernética oficial o documentada

- Desarrollo de la estrategia
- Organización
- Contenido

Defensa cibernética

- Estrategia
- Organización
- Coordinación

Cultura y sociedad

Mentalidad de seguridad cibernética

- En el gobierno
- En el sector privado
- En la sociedad

Conciencia de seguridad cibernética

- Sensibilización

Confianza en el uso de Internet

- En los servicios en línea
- En el gobierno electrónico
- En el comercio electrónico

Privacidad en línea

- Normas de privacidad
- Privacidad del empleado

Educación

Disponibilidad nacional de la educación y formación cibernéticas

- Educación
- Formación

Desarrollo nacional de la educación de seguridad cibernética

- Desarrollo nacional de la educación de seguridad cibernética

Formación e iniciativas educativas públicas y privadas

- Capacitación de empleados en seguridad cibernética

Gobernanza corporativa, conocimiento y normas

- Comprensión de la seguridad cibernética por parte de empresas privadas y estatales

Marcos legales

Marcos jurídicos de seguridad cibernética

- Para la seguridad de las TIC
- Privacidad, protección de datos y otros derechos humanos
- Derecho sustantivo de delincuencia cibernética
- Derecho procesal de delincuencia cibernética

Investigación jurídica

- Cumplimiento de la ley
- La fiscalía
- Tribunales

Divulgación responsable de la información

- Divulgación responsable de la información

Tecnologías

Adhesión a las normas

- Aplicación de las normas y prácticas mínimas aceptables
- Adquisiciones
- Desarrollo de softwre

Organizaciones de coordinación de seguridad cibernética

- Centro de mando y control
- Capacidad de respuesta a incidentes

Respuesta a incidentes

- Identificación y designación
- Organización
- Coordinación

Resiliencia de la infraestructura nacional

- Infraestructura tecnológica
- Resiliencia nacional

Protección de la Infraestructura Crítica Nacional (ICN)

- Identificación
- Organización
- Planeación de respuesta
- Coordinación
- Gestión de riesgos

Gestión de crisis

- Planeación
- Evaluación

Redundancia digital

- Planeación
- Organización

Mercado de la ciberseguridad

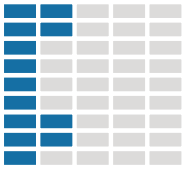
- Tecnologías de seguridad cibernética
- Seguros de delincuencia cibernética

.sr

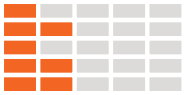
Suriname

Política y estrategia

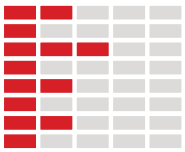
Cultura y sociedad



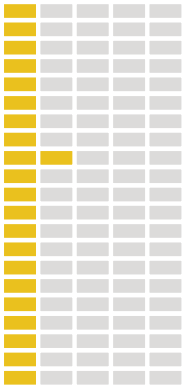
Educación



Marcos legales



Tecnología



En la 69ª Sesión de la Asamblea General de la ONU en octubre de 2014, un representante de la Misión Permanente de Suriname habló en nombre de los Estados de América del Sur y enfatizó la importancia de proteger la infraestructura crítica de las amenazas cibernéticas, mientras se preservan los derechos de los ciudadanos a la información y la privacidad[36]. Aunque Suriname no ha sido históricamente un objetivo común para los ataques cibernéticos, crecientes amenazas de seguridad cibernética en la región llevaron a su gobierno, alrededor del año 2012, a comenzar a desarrollar una estrategia nacional y restaurar su actualmente desaparecido Equipo de Respuesta a Incidentes de Seguridad Informática nacional, SurCSIRT. La Oficina de Seguridad Nacional (BNV), en colaboración con la Agencia Central de Inteligencia y Seguridad (CIVD), tiene la tarea de consultar con las partes interesadas y elaborar la Estrategia Nacional de Seguridad Cibernética, así como restablecer el SurCSIRT. Sin embargo, el avance ha sido lento en cuanto a la respuesta ya que el SurCSIRT aún no está en funcionamiento. Actualmente la principal agencia nacional involucrada en la seguridad cibernética es la CIVD, que investiga los ataques cibernéticos, proporciona información a la policía nacional y trabaja en estrecha colaboración con el sector privado. Según las autoridades el gobierno en su conjunto tiene un conocimiento limitado de las cuestiones de seguridad cibernética. En el ámbito de la defensa cibernética, la Política de Defensa Nacional del Ministerio de Defensa incluye medidas relacionadas con la seguridad de las TIC.

Si bien Suriname tiene leyes generales relativas a la privacidad de las personas, no cuenta con un marco legal para hacer frente a los delitos cibernéticos. La Fiscalía General es el principal responsable para el manejo de casos nacionales de delincuencia cibernética. Aunque las autoridades de justicia penal tienen cierta capacidad, la falta de servicios forenses digitales o mecanismos de información responsables supone un gran reto para el enjuiciamiento efectivo de los delitos cibernéticos.

Las partes interesadas del sector privado y de la Infraestructura Crítica Nacional (ICN) están cada vez más preocupados por su nivel de seguridad cibernética. El gobierno mantiene un listado general de los activos y vulnerabilidades de la ICN y las empresas privadas, especialmente en los sectores bancario y de telecomunicaciones, están discutiendo medidas de protección de privacidad e invirtiendo en formación de los empleados en seguridad cibernética. Del mismo modo estas industrias tienden a cumplir con las normas ISO 27001 y se proponen crear conciencia entre otros sectores. Si bien las medidas de redundancia digitales no están en marcha en todas las entidades, estas se han implementado en Puntos de Intercambio de Internet (IXP).

Sin embargo la conciencia social de la seguridad cibernética es generalmente baja, ya que no ha habido campañas nacionales y el 40% de la población está conectada a Internet[37]. Además existen pocas oportunidades de educación en el país para los ciudadanos interesados en trabajar en la seguridad cibernética.

POBLACIÓN TOTAL DEL PAÍS	**538.248**
Abonos a teléfonos celulares	927.800
Personas con acceso a Internet	215.299

Penetración de Internet

40%

Política y estrategia

Estrategia nacional de seguridad cibernética oficial o documentada

- Desarrollo de la estrategia
- Organización
- Contenido

Defensa cibernética

- Estrategia
- Organización
- Coordinación

Cultura y sociedad

Mentalidad de seguridad cibernética

- En el gobierno
- En el sector privado
- En la sociedad

Conciencia de seguridad cibernética

- Sensibilización

Confianza en el uso de Internet

- En los servicios en línea
- En el gobierno electrónico
- En el comercio electrónico

Privacidad en línea

- Normas de privacidad
- Privacidad del empleado

Educación

Disponibilidad nacional de la educación y formación cibernéticas

- Educación
- Formación

Desarrollo nacional de la educación de seguridad cibernética

- Desarrollo nacional de la educación de seguridad cibernética

Formación e iniciativas educativas públicas y privadas

- Capacitación de empleados en seguridad cibernética

Gobernanza corporativa, conocimiento y normas

- Comprensión de la seguridad cibernética por parte de empresas privadas y estatales

Marcos legales

Marcos jurídicos de seguridad cibernética

- Para la seguridad de las TIC
- Privacidad, protección de datos y otros derechos humanos
- Derecho sustantivo de delincuencia cibernética
- Derecho procesal de delincuencia cibernética

Investigación jurídica

- Cumplimiento de la ley
- La fiscalía
- Tribunales

Divulgación responsable de la información

- Divulgación responsable de la información

Tecnologías

Adhesión a las normas

- Aplicación de las normas y prácticas mínimas aceptables
- Adquisiciones
- Desarrollo de softwre

Organizaciones de coordinación de seguridad cibernética

- Centro de mando y control
- Capacidad de respuesta a incidentes

Respuesta a incidentes

- Identificación y designación
- Organización
- Coordinación

Resiliencia de la infraestructura nacional

- Infraestructura tecnológica
- Resiliencia nacional

Protección de la Infraestructura Crítica Nacional (ICN)

- Identificación
- Organización
- Planeación de respuesta
- Coordinación
- Gestión de riesgos

Gestión de crisis

- Planeación
- Evaluación

Redundancia digital

- Planeación
- Organización

Mercado de la ciberseguridad

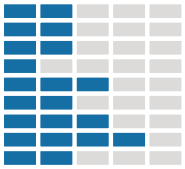
- Tecnologías de seguridad cibernética
- Seguros de delincuencia cibernética

.tt

Trinidad y Tobago

Política y estrategia

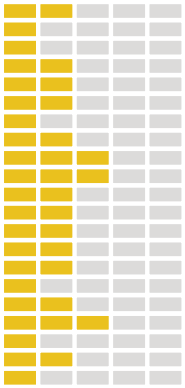
Cultura y sociedad



Educación

Marcos legales

Tecnología



Con una tasa de penetración de Internet de 65% en 2014, frente a 48,5% en 2010, el Gobierno de Trinidad y Tobago se ha dedicado activamente a que se acepten las TIC, se protejan sus activos digitales y se fomente el desarrollo económico a través de la articulación de una estrategia nacional de seguridad cibernética, la identificación de una autoridad competente y el establecimiento de las capacidades de respuesta a incidentes cibernéticos.

En respuesta a una serie de ataques cibernéticos en 2011, el Marco de Políticas de Mediano Plazo de Trinidad y Tobago reconoció oficialmente tanto el papel que desempeñan las TIC en la promoción del desarrollo y el crecimiento económico nacional como la necesidad de implementar iniciativas efectivas de seguridad cibernética para proteger esta infraestructura central[38]. En diciembre de 2012 el Ministerio de Seguridad Nacional publicó una estrategia integral nacional que detalla los riesgos cibernéticos del país y establece las funciones y responsabilidades de las entidades. Si bien no existe una política de defensa cibernética aprobada, el J6 dentro de la Fuerza de Defensa de Trinidad y Tobago (TTDF, por sus siglas en inglés) tiene la responsabilidad general de los asuntos de las TIC y de defensa cibernética. Además existen funcionarios de las TI dentro de las formaciones de la TTDF (Regimiento, Guardia Costera y Guardia Aérea) que comparten responsabilidades de defensa cibernética. Este año, Trinidad y Tobago lanzará oficialmente el primer Equipo Nacional de Respuesta a Incidentes de Seguridad Informática del país, TTCSIRT. El equipo trabajará en estrecha colaboración con la OEA, la Unión Internacional de Telecomunicaciones y otras organizaciones internacionales para desarrollar la capacidad de respuesta a incidentes.

Muchos propietarios y operadores de la Infraestructura Crítica Nacional (ICN) cuentan con mecanismos de respuesta o información de crisis en marcha, en particular aquellos en el sector privado.

La Estrategia Nacional de Seguridad Cibernética requiere la construcción de competencias entre los principales interesados y el desarrollo de medidas de gestión de incidentes. Por otra parte se está generalizando la adhesión a las normas internacionales como la ISO 27001 en todo el gobierno, con proveedores de telecomunicaciones, servicios de seguridad y sector financiero.

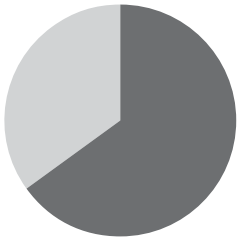
El Ministerio de Seguridad Nacional ha presentado un proyecto de Ley de Delito Cibernético al Parlamento para su promulgación, destinado a derogar la Ley de Uso Indebido de Equipos de Cómputo existente y reemplazarla con un marco jurídico más amplio para atacar la delincuencia cibernética. También existe una Ley de Protección de Datos, pero solo se ha promulgado parcialmente. La Unidad de Delitos Cibernéticos del Servicio de Policía de Trinidad y Tobago se encarga de las investigaciones de delitos cibernéticos y está equipada con un laboratorio forense digital. Sin embargo, puede ser difícil el enjuiciamiento exitoso de delitos cibernéticos ya que los tribunales a menudo carecen de capacidades de gestión de evidencia digital y no hay en operación un marco que le exija al sector privado divulgar incidentes cibernéticos.

El Ministerio de Seguridad Nacional ha puesto en marcha su campaña de concientización pública. Además el Ministerio de Ciencia y Tecnología y diversas organizaciones públicas y privadas, por ejemplo la Universidad de Trinidad y Tobago (UTT) y la Autoridad de Telecomunicaciones de Trinidad y Tobago (TATT) se han asociado para ofrecer talleres y otros programas destinados a educar al público sobre la seguridad cibernética. El sector privado también ha alentado la oferta de formación internacional y programas de acreditación para los empleados. Si bien algunas universidades ofrecen cursos sobre hacking ético, actualmente no hay ningún programa nacional de grado o de certificados en seguridad cibernética.

POBLACIÓN TOTAL DEL PAÍS	**1.354.483**
Abonos a teléfonos celulares	1.980.566
Personas con acceso a Internet	880.414

Penetración de Internet

65%



Política y estrategia

Estrategia nacional de seguridad cibernética oficial o documentada

- Desarrollo de la estrategia
- Organización
- Contenido

Defensa cibernética

- Estrategia
- Organización
- Coordinación

Cultura y sociedad

Mentalidad de seguridad cibernética

- En el gobierno
- En el sector privado
- En la sociedad

Conciencia de seguridad cibernética

- Sensibilización

Confianza en el uso de Internet

- En los servicios en línea
- En el gobierno electrónico
- En el comercio electrónico

Privacidad en línea

- Normas de privacidad
- Privacidad del empleado

Educación

Disponibilidad nacional de la educación y formación cibernéticas

- Educación
- Formación

Desarrollo nacional de la educación de seguridad cibernética

- Desarrollo nacional de la educación de seguridad cibernética

Formación e iniciativas educativas públicas y privadas

- Capacitación de empleados en seguridad cibernética

Gobernanza corporativa, conocimiento y normas

- Comprensión de la seguridad cibernética por parte de empresas privadas y estatales

Marcos legales

Marcos jurídicos de seguridad cibernética

- Para la seguridad de las TIC
- Privacidad, protección de datos y otros derechos humanos
- Derecho sustantivo de delincuencia cibernética
- Derecho procesal de delincuencia cibernética

Investigación jurídica

- Cumplimiento de la ley
- La fiscalía
- Tribunales

Divulgación responsable de la información

- Divulgación responsable de la información

Tecnologías

Adhesión a las normas

- Aplicación de las normas y prácticas mínimas aceptables
- Adquisiciones
- Desarrollo de softwre

Organizaciones de coordinación de seguridad cibernética

- Centro de mando y control
- Capacidad de respuesta a incidentes

Respuesta a incidentes

- Identificación y designación
- Organización
- Coordinación

Resiliencia de la infraestructura nacional

- Infraestructura tecnológica
- Resiliencia nacional

Protección de la Infraestructura Crítica Nacional (ICN)

- Identificación
- Organización
- Planeación de respuesta
- Coordinación
- Gestión de riesgos

Gestión de crisis

- Planeación
- Evaluación

Redundancia digital

- Planeación
- Organización

Mercado de la ciberseguridad

- Tecnologías de seguridad cibernética
- Seguros de delincuencia cibernética

.uy

Uruguay

Política y estrategia

Cultura y sociedad

Educación

Marcos legales

Tecnología

En 2014, Uruguay tenía una alta tasa de penetración de las TIC de 61%, que ha ido en constante aumento a partir de un 46,4% en 2010[39]. El Gobierno de Uruguay ha buscado aumentar la adopción de las TIC y proteger sus activos de información a través de políticas de seguridad cibernética, la capacidad de respuesta a incidentes, capacitación y desarrollo del personal, y legislación, y así ayudar a impulsar la economía de Uruguay hacia la era de la información.

Mediante el Decreto Presidencial 452/009, el Gobierno de Uruguay requirió que todas las entidades gubernamentales desarrollen políticas de seguridad cibernética. Uruguay no tiene una estrategia nacional específica para la seguridad cibernética, pero la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento (AGESIC) incluyó el tema de seguridad cibernética en su Agenda Digital quinquenal para 2011-2015, y enfatizará aún más la seguridad cibernética en el próximo plan a 5 años[40]. Por otra parte, la Política de Defensa Nacional de Uruguay incorpora medidas de defensa cibernética. El mecanismo nacional de respuesta a incidentes de seguridad informática del país, el CERTuy establecido en 2008, coordina regularmente con otros CSIRT regionales y organizaciones internacionales. Además de respuesta a incidentes, el CERTuy suministra registros estadísticos sobre ataques cibernéticos y emite alertas sobre riesgos emergentes. Uruguay también se basa en el análisis y la respuesta de incidentes del CSIRT-ANTEL de la Administración Nacional de Telecomunicaciones, que fue fundada en 2005 para abordar cuestiones relacionadas con los datos y servicios de telefonía celular.

El Gobierno de Uruguay maneja formalmente la seguridad de la Infraestructura Crítica Nacional (ICN) y comparte información sobre sus activos y vulnerabilidades. También refuerza las normas de seguridad y de privacidad del empleado. Uruguay es líder regional en el desarrollo de software de seguridad y un mercado de nuevas tecnologías y seguro contra la delincuencia cibernética. Las entidades gubernamentales también ejecutan ejercicios de gestión del riesgo para coordinar eficazmente los activos de respuesta. En casos de emergencia, el Sistema Nacional de Emergencias emitiría una comunicación de redundancia.

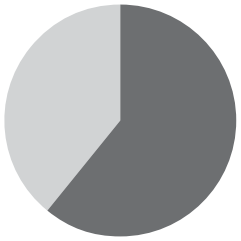
La Unidad de Delitos Cibernéticos de la Policía Nacional es el organismo responsable de la investigación de los delitos cibernéticos. Recibe capacitación de la OEA y otras organizaciones, y mantiene un laboratorio forense digital. En los últimos años la unidad ha detectado un aumento de la delincuencia cibernética. El Gobierno de Uruguay ha elaborado un marco jurídico para la seguridad cibernética y ha adoptado la Ley n° 18.331 de Protección de Datos. Sin embargo no ha adoptado una legislación penal específica para los delitos informáticos y no cuenta con ningún mecanismo de divulgación para el sector privado. Uruguay forma parte del Mercosur Digital que tiene como objetivo normalizar el comercio electrónico y la seguridad cibernética entre los Estados Miembros. Por otra parte, las principales áreas del sector privado y el sector bancario están bien capacitadas tanto en las amenazas cibernéticas como en las estrategias para protegerse de estas.

La academia y los sectores público y privado ofrecen oportunidades de capacitación y educación en seguridad cibernética y el gobierno ha estado trabajando para mejorar las iniciativas educativas en dicho campo. También ha puesto en marcha campañas nacionales de sensibilización, como "Seguro te conectás", dirigido por el CERTuy, y "Tus datos valen. Cuídalos", dirigido por la AGESIC. Uruguay también se unió a la campaña STOP. THINK.CONNECT. del Departamento de Seguridad Nacional de Estados Unidos.

POBLACIÓN TOTAL DEL PAÍS	**3.419.516**
Abonos a teléfonos celulares	5.497.094
Personas con acceso a Internet	2.085.905

Penetración de Internet

61%



Política y estrategia

Estrategia nacional de seguridad cibernética oficial o documentada

- Desarrollo de la estrategia
- Organización
- Contenido

Defensa cibernética

- Estrategia
- Organización
- Coordinación

Cultura y sociedad

Mentalidad de seguridad cibernética

- En el gobierno
- En el sector privado
- En la sociedad

Conciencia de seguridad cibernética

- Sensibilización

Confianza en el uso de Internet

- En los servicios en línea
- En el gobierno electrónico
- En el comercio electrónico

Privacidad en línea

- Normas de privacidad
- Privacidad del empleado

Educación

Disponibilidad nacional de la educación y formación cibernéticas

- Educación
- Formación

Desarrollo nacional de la educación de seguridad cibernética

- Desarrollo nacional de la educación de seguridad cibernética

Formación e iniciativas educativas públicas y privadas

- Capacitación de empleados en seguridad cibernética

Gobernanza corporativa, conocimiento y normas

- Comprensión de la seguridad cibernética por parte de empresas privadas y estatales

Marcos legales

Marcos jurídicos de seguridad cibernética

- Para la seguridad de las TIC
- Privacidad, protección de datos y otros derechos humanos
- Derecho sustantivo de delincuencia cibernética
- Derecho procesal de delincuencia cibernética

Investigación jurídica

- Cumplimiento de la ley
- La fiscalía
- Tribunales

Divulgación responsable de la información

- Divulgación responsable de la información

Tecnologías

Adhesión a las normas

- Aplicación de las normas y prácticas mínimas aceptables
- Adquisiciones
- Desarrollo de softwre

Organizaciones de coordinación de seguridad cibernética

- Centro de mando y control
- Capacidad de respuesta a incidentes

Respuesta a incidentes

- Identificación y designación
- Organización
- Coordinación

Resiliencia de la infraestructura nacional

- Infraestructura tecnológica
- Resiliencia nacional

Protección de la Infraestructura Crítica Nacional (ICN)

- Identificación
- Organización
- Planeación de respuesta
- Coordinación
- Gestión de riesgos

Gestión de crisis

- Planeación
- Evaluación

Redundancia digital

- Planeación
- Organización

Mercado de la ciberseguridad

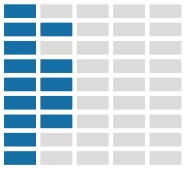
- Tecnologías de seguridad cibernética
- Seguros de delincuencia cibernética

.ve

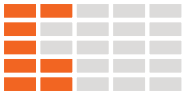
Venezuela

Política y estrategia

Cultura y sociedad

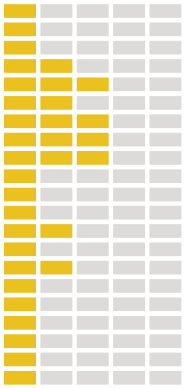


Educación



Marcos legales

Tecnología



La entidad líder de Venezuela para la seguridad cibernética nacional, el Sistema Nacional de Gestión de Incidentes Telemáticos (conocido como VenCERT), realiza múltiples funciones, a saber: respuesta a incidentes cibernéticos, mantenimiento de estadísticas sobre tendencias de ataques cibernéticos, y evaluación y fortalecimiento de la infraestructura nacional de seguridad cibernética. A medida que los ataques cibernéticos siguen en aumento en el país, incluyendo atentados contra sitios web gubernamentales y ataques de denegación de servicio distribuidos (DdoS), la capacidad de respuesta del VenCERT se ha visto limitada[41]. Recientemente ha aumentado su personal, pero requiere nuevas técnicas y herramientas para mantenerse vigente con las amenazas informáticas emergentes.

Venezuela no tiene ni una política nacional de seguridad cibernética ni una estrategia de defensa cibernética. No obstante, ha aprobado una serie de leyes que en conjunto constituyen un marco jurídico global para la delincuencia cibernética. La Ley Especial contra los Delitos Informáticos (Ley 37.313) fue promulgada en 2001, y la Asamblea Nacional ha promulgado recientemente la Ley de Interoperabilidad (2012) y la Ley de Infogobierno (2013), que establecen reglas y normas para el intercambio electrónico, así como pautas del derecho procesal. Aunque la Constitución establece la libertad de expresión, no hay leyes en vigor que traten específicamente sobre la privacidad o la libertad de expresión en línea.

Tres entidades conforman la respuesta principal del país contra la delincuencia cibernética: el Cuerpo de Investigaciones Científicas, Penales y Criminalísticas (CICPC), el Centro Nacional de Informática Forense (CENIF) y la Superintendencia de Servicios de Certificación Electrónica (SUSCERTE). El gobierno ofrece rutinariamente capacitación al personal del CICPC para asegurarse de que esté al día en las tendencias de la delincuencia cibernética.

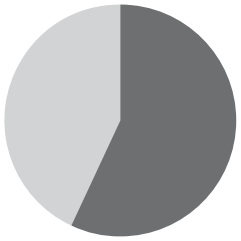
A través de su plan de Patria Segura, el SUSCERTE gestiona formalmente la seguridad de la tecnología de la Infraestructura Crítica Nacional (ICN), emite certificados digitales y mantiene estadísticas sobre incidentes. Los operadores de la ICN han comenzado a adoptar medidas de seguridad para cumplir con las normas internacionales y tienen capacidad básica para proteger la infraestructura de los ataques cibernéticos.

Además de la emisión de certificados digitales para el gobierno y tecnología de la ICN y el mantenimiento de estadísticas, el SUSCERTE ha liderado la campaña "La seguridad de la información comienza por ti", que tiene como objetivo educar al público sobre la seguridad cibernética a través de charlas, foros y talleres. También están disponibles en el país una serie de programas de grado sobre seguridad cibernética y delincuencia cibernética. Sin embargo la falta de conciencia social sobre seguridad cibernética y la limitada protección de la privacidad de los ciudadanos aún presenta desafíos al régimen de seguridad cibernética de Venezuela.

POBLACIÓN TOTAL DEL PAÍS	**30.693.827**
Abonos a teléfonos celulares	30.528.022
Personas con acceso a Internet	17.495.481

Penetración de Internet

57%



Política y estrategia

Estrategia nacional de seguridad cibernética oficial o documentada

- Desarrollo de la estrategia
- Organización
- Contenido

Defensa cibernética

- Estrategia
- Organización
- Coordinación

Cultura y sociedad

Mentalidad de seguridad cibernética

- En el gobierno
- En el sector privado
- En la sociedad

Conciencia de seguridad cibernética

- Sensibilización

Confianza en el uso de Internet

- En los servicios en línea
- En el gobierno electrónico
- En el comercio electrónico

Privacidad en línea

- Normas de privacidad
- Privacidad del empleado

Educación

Disponibilidad nacional de la educación y formación cibernéticas

- Educación
- Formación

Desarrollo nacional de la educación de seguridad cibernética

- Desarrollo nacional de la educación de seguridad cibernética

Formación e iniciativas educativas públicas y privadas

- Capacitación de empleados en seguridad cibernética

Gobernanza corporativa, conocimiento y normas

- Comprensión de la seguridad cibernética por parte de empresas privadas y estatales

Marcos legales

Marcos jurídicos de seguridad cibernética

- Para la seguridad de las TIC
- Privacidad, protección de datos y otros derechos humanos
- Derecho sustantivo de delincuencia cibernética
- Derecho procesal de delincuencia cibernética

Investigación jurídica

- Cumplimiento de la ley
- La fiscalía
- Tribunales

Divulgación responsable de la información

- Divulgación responsable de la información

Tecnologías

Adhesión a las normas

- Aplicación de las normas y prácticas mínimas aceptables
- Adquisiciones
- Desarrollo de softwre

Organizaciones de coordinación de seguridad cibernética

- Centro de mando y control
- Capacidad de respuesta a incidentes

Respuesta a incidentes

- Identificación y designación
- Organización
- Coordinación

Resiliencia de la infraestructura nacional

- Infraestructura tecnológica
- Resiliencia nacional

Protección de la Infraestructura Crítica Nacional (ICN)

- Identificación
- Organización
- Planeación de respuesta
- Coordinación
- Gestión de riesgos

Gestión de crisis

- Planeación
- Evaluación

Redundancia digital

- Planeación
- Organización

Mercado de la ciberseguridad

- Tecnologías de seguridad cibernética
- Seguros de delincuencia cibernética

Notas de los perfiles de países

1. Grupo del Banco Mundial, "Internet users (per 100 people)," World DataBank (2015), web, **http://data.worldbank.org/indicator/IT.NET.USER.P2**.

2. Gobierno de Antigua y Barbuda, "Ministry holds Cyber Security Awareness Workshop for Employees", comunicado de prensa, Ministerio de Información, St. John's, 05 de enero de 2012, **http://www.ab.gov.ag/article_details.php?id=2438&category=38**.

3. Organización de los Estados Americanos, "OAS Assists Bahamas in the Development of a National Cyber Security Strategy", comunicado de prensa no. 173/14, 30 de abril de 2014, consultado el 13 de noviembre de 2015, **https://www.oas.org/en/media_center/press_release.asp?sCodigo=E-173/1**.

4. Dennis Adonis, "Bahamas to get ethical hacking and cyber security training, in wake of cyber attacks," Jewish Journal, (Los Angeles, CA), 16 de mayo de 2015.

5. Barbados Nation, "BGIS website hacked," Nation News (Bridgetown, Barbados), 01 de junio de 2015.

6. Grupo del Banco Mundial, "Internet users (per 100 people)," World DataBank (2015), web, **http://data.worldbank.org/indicator/IT.NET.USER.P2**.

7. Grupo del Banco Mundial, "Internet users (per 100 people)," World DataBank (2015), web, **http://data.worldbank.org/indicator/IT.NET.USER.P2**.

8. Agencia para el Desarrollo de la Sociedad de la Información en Bolivia, "Misión y Visión", ADSIB, 2011, consultado el 18 de junio 2015, **http://www.adsib.gob.bo/adsibnueva/mision_vision.php**.

9. Data Center Map, "PIT-BOLIVIA - Punto de Intercambio de Tráfico - Bolivia" Data Center Research, consultado 18 de junio 2015, **http://www.datacentermap.com/ixp/pit-bolivia.html**. Los IXP son estructuras físicas que canalizan y ofrecen contenido de Internet más rápido, y conectividad más segura a un menor costo.

10. N.A., "Rio Builds a high tech integrated urban command center", Homeland Security News Wire, 30 de mayo de 2014, consultado el 5 de octubre de 2015, **http://www.homelandsecuritynewswire.com/dr20140530-rio-builds-a-high-tech-integrated-urban-command-center.**

11. Departamento de Seguridad de la Información y las Comunicaciones, "Estratégia de Segurança da Informação e Comunicações (SIC) e de Segurança Cibernética da Administração Pública Federal (APF), " 26 de mayo de 2015, **http://dsic.planalto.gov.br/documentos/publicacoes/4_Estrategia_de_SIC.pdf.**

12. Comité Gestor de Internet de Brasil, "About the CGI.br", CGI.br, visitado el 17 de agosto de 2015, **http://cgi.br/about/.**

13. Freedom House, "Ecuador", Freedom on the Net 2014, web, consultado 08 de junio 2015, web, **https://freedomhouse.org/report/freedom-world/2014/ecuador**

14. Grupo del Banco Mundial, "Internet users (per 100 people)," World DataBank (2015), web, **http://data.worldbank.org/indicator/IT.NET.USER.P2**.

15. CARICOM, Granada Calls for More Support for the Region's ICT Initiatives, comunicado de prensa, Secretaría de la Comunidad del Caribe, 21 de julio de 2012, **http://www.caricom.org/jsp/pressreleases/press_releases_2012/pres200_12.jsp**.

16. Guillermo Isaí Ramírez, "Gobierno se Defiende del ataque de Anonymus," Prensa Libre 2 de mayo de 2015, web, consultado el 19 de junio 2015, **http://www.prensalibre.com/economia/gobierno-se-defiende-del-ataque-de-anonymus**.

17. Grupo del Banco Mundial, "Internet users (per 100 people)," World Databank (2015), web, **http://data.worldbank.org/indicator/IT.NET.USER.P2**.

18. Autor desconocido, "Guyana Moves to Tackle Cybercrime", Kaieteur News, 13 de agosto de 2015, consultado el 15 de noviembre de 2015, **http://www.kaieteurnewsonline.com/2015/08/13/guyana-moves-to-tackle-cyber-crime/.**

19. CSIRT-GY, "National Cyber Security Sensitisation Workshop 2015", CSIRT-GY, 10 de agosto de 2015, web, consultado el 18 de agosto de 2015, **http://www.CSIRT.gy/event/ncssw-2015**.

20. Amelie Baron, "Haiti enters uncertain political phase as parliament dissolved," Reuters, Port-Au-Prince, 13 de enero de 2015, web, consultado el 19 de junio de 2015, **http://www.reuters.com/article/2015/01/13/us-haiti-parliament-idUSKBN0KM2CX20150113**.

21. Grupo del Banco Mundial, "Internet users (per 100 people)," World DataBank (2015), web, **http://data.worldbank.org/indicator/IT.NET.USER.P2**.

22. Grupo del Banco Mundial, "Internet users (per 100 people)," World DataBank (2015), web, **http://data.worldbank.org/indicator/IT.NET.USER.P2**.

23. Autor desconocido, "OAS To Assist Government Following Cyber Attacks," The Gleaner, Kingston, Jamaica, 17 de diciembre de 2014, web, consultado el 19 de junio de 2015, **http://jamaica-gleaner.com/article/20141217/oas-assist-government-following-cyber-attacks**.

24. Grupo del Banco Mundial, "Internet users (per 100 people)," World Data-Bank (2015), web, **http://data.worldbank.org/indicator/IT.NET.USER.P2**.

25. ESET, ESET Security Report Latinoamérica 2014 (Buenos Aires: ESET Latinoamérica, 2014).

26. N.A. "Inauguran semana del uso seguro de Internet," El Nuevo Diario, Managua, Nicaragua, 25 de mayo de 2015, web, consultado el 19 de junio, 2015, **http://www.elnuevodiario.com.ni/nacionales/360817-inauguran-semana-uso-seguro-Internet/**.

27. Grupo del Banco Mundial, "Internet users (per 100 people)," World DataBank (2015), web, **http://data.worldbank.org/indicator/IT.NET.USER.P2**.

28. Mariela Mejía, "Ataques 'phishing' desviaron más de RD $120 millones de bancos," Diario Libre, 12 de febrero de 2014, web, consultado el 19 de junio 2015, **http://www.diariolibre.com/destacada/2014/02/12/i478961_ataques-phishing-desviaron-rd120-millones-bancos.html**.

29. Grupo del Banco Mundial, "Internet users (per 100 people)," World DataBank (2015), web, **http://data.worldbank.org/indicator/IT.NET.USER.P2**.

30. N.A. "St Kitts and Nevis to host ICT Week," Caribbean News Now, Basseterre, St Kitts, septiembre de 2014, web, consultado el 24 de junio de 2015, **http://www.caribbeannewsnow.com/headline-St-Kitts-and-Nevis-to-host-ICT-Week-22628.html**.

31. Grupo del Banco Mundial, "Internet users (per 100 people)," World DataBank (2015), web, **http://data.worldbank.org/indicator/IT.NET.USER.P2**.

32. Gobierno de San Vicente y las Granadinas, "One Laptop Per Student," Gov.vc, web, consultado el 24 de junio de 2015, **http://www.gov.vc/index.php?option=com_content&view=article&id=349%3Aone-laptop-per-student&Itemid=159**.

33. N.A. "St Lucia gov't moving to strengthen cyber-security," Jamaica Observer, Castries, St Lucia (CMC), 06 de mayo de 2015, web, consultado el 24 de junio

de 2015, **http://www.jamaicaobserver.com/latestnews/St-Lucia-gov-t-moving-to-strengthen-cyber-security**.

34. Bankers Association of St. Lucia Inc., "Bankers Association Supports Police Cyber Crime Efforts," BASLU, N.D., web, consultado el 24 de junio de 2015, **http://baslu.org/portofolio/maecenas-nec-eros-lacus/**.

35. Michele Marius, "3 emerging trends in Caribbean Internet Governance policy," ICT Pulse, 12 de septiembre de 2012, web, consultado, **http://www.ict-pulse.com/2012/09/3-emerging-trends-caribbean-Internet-governance-policy/**.

36. Asamblea General de las Naciones Unidas, "Cyber Warfare, Unchecked, Could Topple Entire Edifice of International Security, Says Speaker in First Committee at Conclusion of Thematic Debate Segment," Sixty-ninth session, 19th Meeting (PM), Meetings Coverage, 28 de octubre de 2014, web, consultado el 24 de junio de 2015, **http://www.un.org/press/en/2014/gadis3512.doc.htm**.

37. Grupo del Banco Mundial, "Internet users (per 100 people)," World DataBank (2015), web, **http://data.worldbank.org/indicator/IT.NET.USER.P2**.

38. Andre Bagoo, "Cyber crime wave," Newsday, 08 de julio de 2012, web, consultado el 24 de junio de 2015, **http://www.newsday.co.tt/politics/0,162969.html**.

39. "Internet users (per 100 people)". Banco Mundial. consultado el 22 de july de 2015. Web. Recuperado de **http://data.worldbank.org/indicator/IT.NET.USER.P2**

40. Gobierno de Uruguay, "Estrategia y Agenda Digital," Mapa de ruta: Agenda Digital Uruguay 2011-2015, Montevideo, Uruguay, web, consultado el 24 de junio 2015, **http://www.agesic.gub.uy/innovaportal/v/1443/1/agesic/mapa_de_ruta:_agenda_digital_uruguay_2011-2015.html?menuderecho=11**.

41. N.A. "Más de 127 ataques cibernéticos con fines políticos en Venezuela," Telesur, 17 de febrero de 2014, web, consultado en junio 24 de 2015, **http://www.telesurtv.net/news/Mas-de-127-ataques-ciberneticos-con-fines-politicos-en-Venezuela-20140217-0014.html**.

Reflexiones sobre la región

Melissa Hathaway, Jennifer McArdle y Francesca Spidalieri

Las regiones de América Latina y Caribe (ALC) están acelerando su enfoque en la seguridad cibernética y lo están priorizando en su agenda social y de política. Los líderes del gobierno no pueden ignorar el hecho de que los incidentes de seguridad cibernética están aumentando, tanto en alcance como en su escala. Reconociendo su responsabilidad con su país y los ciudadanos, deben tomar las medidas y hacer las inversiones necesarias para abordar la resiliencia de los servicios e infraestructuras básicas de su país y poder recuperarse rápidamente de los incidentes cibernéticos, mientras continúan acogiendo las oportunidades que se presentan al tener una sociedad conectada.

Los 32 países participantes tienen diferentes enfoques, actitudes y prioridades en cuanto a la seguridad cibernética. Las siguientes observaciones de alto nivel muestran las tendencias en la región.

1. Los gobiernos reconocen la importancia de asegurar el acceso asequible a los servicios de la tecnología de la información y las comunicaciones (TIC) para la innovación empresarial, el crecimiento y la prestación de servicios públicos. Sin embargo, la penetración de Internet es todavía muy baja (un promedio de menos del 50%) en aproximadamente la mitad de la región de ALC. Iniciativas de desarrollo económico de toda la región están pidiendo inversiones de banda ancha y modernización de la infraestructura para impulsar a sus países hacia la era digital.

2. La adopción de una estrategia de seguridad cibernética nacional es posiblemente uno de los elementos más importantes del compromiso de un país en asegurar la infraestructura cibernética, servicios y ambiente de negocios de los que dependen su futuro digital y el bienestar económico. Algunos países de ALC le han dado prioridad a la seguridad cibernética como una preocupación nacional y están estableciendo políticas formales de seguridad cibernética y construyendo las capacidades de organismos pertinentes. Hasta la fecha, solo seis países de la región han adoptado estrategias de seguridad cibernética: Brasil, Colombia, Jamaica, Panamá, Trinidad y Tobago y Uruguay. Otros países, entre ellos Argentina, Antigua y Barbuda, Bahamas, Costa Rica, Dominica, El Salvador, Haití, México, Paraguay, Perú y Suriname, se encuentran actualmente adelantando la articulación de una estrategia potencial.

3. La sociedad, en gran parte, desconoce los riesgos y vulnerabilidades asociadas con el uso de las TIC. Es importante que los gobiernos describan los riesgos y oportunidades asociadas con el aumento de la conectividad y la dependencia de Internet. Diferentes iniciativas de sensibilización, como las que han comenzado a surgir en muchos países ALC y que han ayudado a construir una comprensión compartida de la importancia de la seguridad cibernética, también pueden conducir a la acción. Dos ejemplos son la campaña "La seguridad de la información comienza por ti" de Venezuela y la campaña internacional STOP. THINK.CONNECT., cuyos objetivos son educar al público sobre los problemas de seguridad cibernética a través de charlas públicas, foros y talleres. Iniciativas como estas son importantes porque pueden aumentar la conciencia de los riesgos cibernéticos inherentes a un país y fomentar el desarrollo de soluciones específicas para aumentar la resiliencia cibernética.

4. El establecimiento de asociaciones público-privadas de confianza y mecanismos formales de intercambio de información sigue siendo limitado en la región. La mayoría de las autoridades nacionales mantienen líneas abiertas y activas de comunicación y colaboración con los sectores críticos y empresas clave, y reconocen la importancia de compartir la inteligencia oportuna y procesable. Sin embargo, la desconfianza entre las partes interesadas ha disminuido la colaboración; y la ausencia de centros reconocidos de intercambios o corredores de información autorizada todavía obstaculiza la capacidad de la mayoría de los países de ALC de establecer mecanismos de intercambio de información formales.

5. La respuesta a las crisis o los mecanismos de presentación de informes están en etapas iniciales en la región, y la capacidad para abordar de manera proactiva las amenazas cibernéticas es limitada. Aproximadamente la mitad de los países de ALC han establecido y operacionalizado Equipos de Respuesta a Incidentes de Seguridad Informática (CSIRT, por sus siglas en inglés; también conocidos como "CERT"). Otros Estados están evaluando los requisitos para montar y poner en práctica este tipo de capacidad. Algunos países, como Colombia, ya tienen iniciativas maduras de respuesta a incidentes y, como tales, pueden proporcionar servicios de respuesta a incidentes de entidades gubernamentales y del sector privado.

6. Los esfuerzos para desarrollar marcos legales integrales para combatir la delincuencia cibernética, un objetivo importante de la estrategia de seguridad cibernética de la OEA, están en marcha en toda la región. Aunque solo dos de los 32 Estados Miembros de la OEA, o sea, la República Dominicana y Panamá, se han adherido a la Convención de Budapest sobre el delito cibernético, casi todos los Estados Miembros han aumentado sus esfuerzos de aplicación de la ley a nivel nacional y han actualizado la legislación nacional para luchar contra el delito cibernético y fortalecer las leyes de protección de datos y privacidad. El enjuiciamiento de los delitos cibernéticos en la región, sin embargo, todavía se ve obstaculizado por la ausencia, en la mayoría de los Estados, de un mecanismo formal para denunciar incidentes cibernéticos. Incluso si se denuncia un incidente, la mayoría de los países cuentan con capacidades

forenses insuficientes para investigar y enjuiciar delitos, o el sistema de justicia penal no ha desarrollado la capacidad de manejar las pruebas electrónicas o hacer cumplir las leyes de delitos informáticos existentes y actualizadas.

7. Algunos gobiernos están aprovechando su mayor conectividad a Internet para explorar oportunidades de desarrollo de tecnología, ampliar su industria interna de tecnología y poner en marcha interesantes programas cibernéticos de investigación y desarrollo (por ejemplo, Start-Up Chile y Visión 2018 de Costa Rica). También han comenzado a ofrecer incentivos, en forma de créditos fiscales, subvenciones y becas para promover el desarrollo de una industria local de tecnología y fomentar la innovación, la educación, la seguridad cibernética, la creación de capacidades y la creación de empleos.

Es alentador que la seguridad cibernética y la resiliencia ocupen un lugar destacado en la política y los programas sociales en América Latina y el Caribe. Si bien ningún país está listo cibernéticamente, muchos están empezando a tomar medidas significativas para evaluar sus desafíos específicos de seguridad cibernética en términos económicos y comprometer recursos limitados para lograr sus objetivos. Si bien sigue habiendo brechas en la preparación para la seguridad cibernética en toda América Latina y el Caribe (como se ve en los resúmenes de las capacidades y los esfuerzos de seguridad cibernética de cada país), la región entera de ALC está avanzando y madurando su compromiso con la creación de una sociedad más segura, resiliente y conectada. ■

Melissa Hathaway

Destacada experta en la política de ciberespacio y ciberseguridad. Es Asesora Principal en el Centro Belfer para la Ciencia y Asuntos Internacionales del Harvard Kennedy School y sirve como Asociada Senior y miembro de la Junta de Regentes en el Instituto Potomac de Estudios Políticos. Se desempeñó en dos administraciones presidenciales, pues estuvo a cargo de la Revista de Política del Ciberespacio para el Presidente Obama y dirigió la Iniciativa Nacional de Seguridad Cibernética Integral para el Presidente George W. Bush. Ha desarrollado una metodología única para evaluar y medir el nivel de preparación para determinados riesgos de ciberseguridad, conocida como el Cyber Readiness Index y está aplicando su metodología para 125 países.

Jennifer McArdle

Investigadora Asociada y miembro del Centro de Pensamiento Científico Revolucionario en el Instituto Potomac de Estudios Políticos, es candidata al doctorado en el Kings College de Londres. Su investigación académica y publicaciones se centran en la seguridad cibernética y problemas de seguridad nacional.

Francesca Spidalieri

Senior Fellow para el Liderazgo Cibernético en el Centro Pell, en Salve Regina University, se desempeña como una experta en la materia en el Proyecto de Cyber Readiness Index del Instituto Potomac de Estudios Políticos. Su investigación académica y sus publicaciones se han centrado en el desarrollo del liderazgo cibernético, la gestión de riesgos cibernéticos, la educación y la conciencia cibernética, y el desarrollo del personal de seguridad cibernética.

Contribuciones

El Banco Interamericano de Desarrollo (BID) y la Organización de los Estados Americanos (OEA) extienden su más sincero agradecimiento a los expertos e instituciones que han contribuido al Informe 2016 del Observatorio de la Seguridad Cibernética en América Latina y el Caribe. El BID y la OEA reconocen también a las siguientes organizaciones por sus contribuciones a esta iniciativa:

Antigua y Barbuda

- Ministerio de Información
- Oficina del Primer Ministro

Argentina

- Ministerio de Seguridad Nacional
- Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad (ICIC)
- Subsecretaría para la Protección de Infraestructura Crítica y Ciberseguridad

Bahamas

- Fuerza Policial Real de Bahamas
- Ministerio de Seguridad Nacional

Barbados

- Oficina del Procurador General

Belice

- Departamento de Policía de Belice
- Organización Central de Tecnología Informática (CITO)
- Secretaría del Consejo de Seguridad Nacional (NSCS)

Bolivia

- Agencia para el Desarrollo de la Sociedad de la Información en Bolivia (ADSIB)

Brasil

- Agencia Brasileña de Inteligencia (ABIN)
- Centro de Tecnología e Sociedad (CTS) - Fundação Getúlio Vargas
- Comité Gestor de Internet en Brasil (CGI.br)
- Departamento de Seguridad de Información y Comunicaciones, Presidencia de la República de Brasil (DSIC)
- Equipo Nacional de Respuesta ante Incidentes Informáticos de Brasil (CERT.BR)
- Gabinete de Seguridad Institucional de la Presidencia de la República (GSI)
- Instituto de Tecnología e Sociedad (ITS)

Chile

- Ministerio del Interior
- Ministerio de Relaciones Exteriores
- Ministerio de Telecomunicaciones

Colombia

- Asociación Nacional de Empresarios de Colombia (ANDI)
- Cámara Colombiana de Informática y Telecomunicaciones (CCIT)
- .CO Internet
- Fuerzas Armadas
- ISAGEN, EPM
- Ministerio de Defensa Nacional
- Ministerio de Justicia
- Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC)
- Policía Nacional
- UniAndes, Escuela Superior de Guerra, Uniminuto, UPB

Costa Rica

- Instituto Costarricense de Electricidad (ICE)
- Ministerio de Ciencia, Tecnología y Telecomunicaciones (MICITT)
- Ministerio de la Presidencia
- Organismo de Investigación Judicial (OIJ)
- Procuraduría General de la República
- Superintendencia de Telecomunicaciones (SUTEL)
- Universidad de Costa Rica

Dominica

- Asociación de Dominica de Profesionales Tecnología de la Información (DAITP)
- Banco Nacional de Dominica
- Dominica State College
- Ministerio de Información y Telecomunicaciones
- Unidad de Tecnología de Información y Comunicaciones

Ecuador

- ARCOTEL
- Fiscalía General de Ecuador
- Fuerzas Armadas del Ecuador
- Ministerio de Defensa

El Salvador

- Ministerio de Justicia y Seguridad Pública

Granada

- Fuerza de la Policía Real de Granada

Guatemala

- CSIRT-gt
- Ministerio de Gobernación
- Ministerio Público de Guatemala
- Secretaría Técnica del Consejo Nacional de Seguridad
- Superintendencia de Telecomunicaciones

Guyana

- Agencia de Energía de Guyana
- CSIRT.gy
- Fuerza de Defensa de Guyana
- Fuerza de Policía de Guyana
- Ministerio del Interior
- Universidad de Guyana

Haití

- Consejo Nacional de Telecomunicaciones (CONATEL)

Honduras

- Comisión Nacional de Telecomunicaciones (CONATEL)
- COINDIS
- Ministerio de Relaciones Exteriores y Cooperación Internacional
- Policía Nacional de Honduras
- Sistema Nacional de Administración de la Propiedad (SINAP)

Jamaica

- Asociación de Bancos de Jamaica
- Fuerza Policial de Jamaica
- Ministerio de Ciencia, Tecnología, Energía y Minería
- Ministerio Público de Jamaica
- Ministerio de Seguridad Nacional
- Universidad de las Indias Occidentales

México

- Asociación Mexicana de Internet, A.C. (AMIPCI)
- Comité Especializado en la Seguridad de Información (CESI)
- Petróleos Mexicanos
- Procuraduría General de la República (PGR)
- Secretaría de Gobernación

Nicaragua

- Universidad Nacional de Ingeniería

Panamá

- Autoridad del Canal de Panamá
- Autoridad Nacional para la Innovación Gubernamental (AIG)

Paraguay

- Ministerio Público
- Ministerio de Relaciones Exteriores
- Secretaría Nacional de Tecnologías de Información y Comunicaciones (SENATICS)

Perú

- Comando Conjunto Fuerzas Armadas
- Ministerio de Defensa
- Ministerio del Interior del Perú
- Ministerio Público - Fiscalía de la Nación
- Ministerio de Relaciones Exteriores
- Oficina Nacional de Gobierno Electrónico e Información (ONGEI)
- Policía Nacional de Perú

República Dominicana

- Instituto Dominicano de las Telecomunicaciones (INDOTEL)
- Policía Nacional
- Procuraduría General de la República

Saint Kitts y Nevis

- Comisión Reguladora de Servicios Financiaros
- LIME
- Ministerio de Empoderamiento Juvenil, Deportes, Tecnología Informática, Telecomunicaciones y Correo
- Ministerio de Energía, Finanzas, Comercio e Industria
- Policía Real de Saint Kitts y Nevis
- St. Kitts Electricity Company Ltd.

San Vicente y las Granadinas

- Fuerza Policial Real de San Vicente y las Granadinas

Santa Lucía

- Gobierno de Santa Lucia

Suriname

- Agencia Central de Inteligencia y Seguridad (CIVD)
- Banca Red de Suriname
- Cámara de Comercio e Industrias
- DATASUR
- Ministerio de Energía, Finanza, Comercio e Industria
- Oficina del Fiscal General
- Parbonet
- Servicio Especial de Seguridad e Inteligencia (SBID)
- TELESUR

Trinidad y Tobago

- Empresa Nacional de TIC (iGovTT)
- Ministerio de Seguridad Nacional

Uruguay

- Agencia de Gobierno Electrónico, Sociedad de la Información y Conocimiento (AGESIC)
- ANTEL
- Ministerio de Defensa

Venezuela

- Superintendencia de Servicios de Certificación Electrónica (SUSCERTE)

El reconocimiento a las instituciones mencionadas anteriormente no implica que las mismas validen el contenido del presente documento.

Apéndice

Marco metodológico detallado

Política y estrategia

Estrategia nacional de seguridad cibernética oficial o documentada
Desarrollo de la estrategia
Organización
Contenido

Defensa cibernética
Estrategia
Organización
Coordinación

Estrategia nacional de seguridad cibernética oficial o documentada

Una estrategia nacional integral de seguridad cibernética identifica los intereses y roles de una gama de actores que contribuyen a, tienen la responsabilidad de o se ven afectadas por la seguridad cibernética con el propósito de crear un marco coordinado y cohesionado. Esta estrategia en ocasiones incluye varias áreas temáticas e identifica los roles y responsabilidades de varios actores que participan en la seguridad cibernética, incluida la industria, la sociedad civil y personas naturales, y destacará la importancia de los mecanismos para abordar sus necesidades y aprovechar su experiencia.

Desarrollo de la estrategia

INICIAL

No hay evidencia de la existencia de una estrategia nacional de seguridad cibernética; si existe un componente cibernético, puede ser responsabilidad de uno o más departamentos del gobierno; ha comenzado un proceso para el desarrollo sin consultar a los interesados.

FORMATIVO

Se ha articulado un esquema de una estrategia nacional de seguridad cibernética construido sobre la base de la consulta del gobierno; se han establecido procesos de consulta para los grupos de interés clave, posiblemente con asistencia internacional.

ESTABLECIDO

Se ha establecido una estrategia de seguridad cibernética nacional; se ha acordado un mandato específico para consultar a todos los sectores y la sociedad civil; se utilizan tendencias históricas y datos para planificar; una cierta comprensión de los riesgos y amenazas de seguridad cibernética nacional impulsa la creación de capacidades a nivel nacional.

ESTRATÉGICO

La estrategia de seguridad cibernética nacional se implementa con conocimiento por parte de múltiples partes interesadas en todo el gobierno; se confirman los procesos de revisión y renovación de la estrategia; se llevan a cabo ejercicios cibernéticos regulares de escenario y en tiempo real; planes estratégicos de seguridad cibernética impulsan la creación de capacidad y las inversiones en seguridad; se han establecido procesos de medición y métricas, los cuales se implementan y sirven de base para la toma de decisiones.

DINÁMICO

La estrategia de seguridad cibernética se revisa continuamente para adaptarse a los cambiantes entornos socio-político, de amenazas y tecnológico, impulsando el proceso de toma de decisiones de múltiples partes interesadas; se llevan a cabo medidas de transparencia y de fomento de la confianza (TCBM, por sus siglas en inglés) para garantizar la inclusión y la contribución continua de todos los interesados, incluido el mejoramiento de la asociación público-privada, la sociedad en general y los aliados internacionales.

Organización

INICIAL

No existe una entidad global para la coordinación de la seguridad cibernética; si se cuenta con presupuestos, estos se encuentran en oficinas públicas no relacionadas.

FORMATIVO

Se ha diseñado y difundido un programa de seguridad cibernética coordinado; los presupuestos todavía pueden estar distribuidos; aún es limitada la cooperación interdepartamental.

ESTABLECIDO

Se ha designado un solo programa cibernético dentro de cada entidad gubernamental; existe un dueño departamental o ente coordinador con un presupuesto consolidado; el programa se define, con metas, hitos e indicadores para medir el progreso; se han acordado funciones y responsabilidades claras para las funciones de seguridad cibernética dentro del gobierno.

ESTRATÉGICO

Existen pruebas de la aplicación iterativa de las métricas y el perfeccionamiento resultante de las operaciones y la estrategia a través de los gobiernos involucrados en la seguridad cibernética, incluida la evaluación y gestión del riesgo.

DINÁMICO

Un organismo nacional es designado para difundir e impulsar la aplicación de la estrategia de seguridad cibernética; existe una postura de seguridad cibernética nacional singular con la capacidad de reasignar tareas y presupuestos de forma dinámica de acuerdo con los cambios en la evaluación de riesgos del entorno de seguridad cibernética; se solidifica la cooperación internacional a nivel organizacional.

Contenido

INICIAL

Puede no existir ninguna o puede haber varias estrategias nacionales con una referencia a la seguridad cibernética; si es que existen, el contenido es genérico, no necesariamente alineado con los objetivos nacionales y no proporciona directrices recurribles.

FORMATIVO

El contenido incluye vínculos entre las prioridades nacionales de riesgo y la seguridad cibernética, pero en general son ad hoc y no están detallados.

ESTABLECIDO

El contenido de la estrategia nacional de seguridad cibernética se vincula explícitamente a los riesgos, las prioridades y objetivos nacionales; el contenido incluye la sensibilización al público, la mitigación de la delincuencia cibernética, la capacidad de respuesta a incidentes y la protección de la Infraestructura Crítica Nacional.

ESTRATÉGICO

El contenido de la estrategia nacional de seguridad cibernética se actualiza basándose en los resultados de la aplicación de métricas y mediciones que impulsan la toma de decisiones y guían la inversión de recursos.

DINÁMICO

El contenido de la estrategia se ha modificado en respuesta a las condiciones de seguridad cibernética; se incorpora regularmente al plan estratégico nuevo contenido relativo a los objetivos de seguridad cibernética; se articula el liderazgo y la promoción de un espacio cibernético internacional seguro, resiliente y de confianza.

Defensa cibernética

Puede haber eventos que repercuten en los intereses de seguridad nacional relacionados con la seguridad de la red, la capacidad de recuperación cibernética, la respuesta a incidentes y el intercambio de información, que requieren la participación de los ministerios y organismos de defensa. Por lo tanto, se necesita la preparación de una estrategia que coordine a todas las organizaciones participantes para garantizar un enfoque integrado para hacerle frente a las amenazas a la seguridad nacional. Esta evaluación no pretende examinar la capacidad técnica o militar, sino que se centra en los atributos fácilmente observables, tales como planificación estratégica, organización y coordinación.

Estrategia

INICIAL

Existe una política nacional de seguridad y estrategia de defensa nacional y puede contener un componente de seguridad de la información o digital, pero no existe ninguna política o estrategia de defensa cibernética.

FORMATIVO

Han sido identificadas amenazas específicas a la seguridad nacional en el ciberespacio, tales como actores de amenazas externas, amenazas internas, vulnerabilidades del sistema de suministro y amenazas a la capacidad operativa militar, pero aún no existe una estrategia de respuesta coherente.

ESTABLECIDO

Existe una política nacional de defensa cibernética o un Libro Blanco de defensa cibernética y esboza la posición de los militares en su respuesta a los diferentes tipos y niveles de ataques cibernéticos, incluyendo un conflicto habilitado por la cibernética que produce un efecto convencional, cinético, y ataques cibernéticos ofensivos destinados a perturbar la infraestructura, incluyendo la respuesta a emergencias.

ESTRATÉGICO

La defensa cibernética nacional cumple con el derecho internacional y es compatible con las normas nacionales e internacionales de intervención en el ciberespacio.

DINÁMICO

Se conoce el cambiante panorama de amenazas en la seguridad cibernética mediante la revisión constante para cerciorarse de que las políticas de defensa cibernética continúen cumpliendo con los objetivos de seguridad nacional; están claramente definidas las normas de intervención; la doctrina militar que se aplica al ciberespacio está completamente desarrollada y toma nota de los cambios significativos en el entorno de la seguridad cibernética.

Organización

INICIAL

No hay gestión de la defensa cibernética; si es que existe, puede ser distribuida entre las fuerzas armadas y/o algunas otras organizaciones gubernamentales; no hay una estructura de mando clara para la seguridad cibernética en las fuerzas armadas.

FORMATIVO

Las unidades de operación de defensa cibernética se incorporan a las diferentes ramas de las fuerzas armadas, pero no existe una estructura central de mando y control.

ESTABLECIDO

Dentro del ministerio responsable de la defensa, existe una organización definida para enfrentar los conflictos utilizando medios cibernéticos.

ESTRATÉGICO

Se integran a la estrategia de defensa nacional la experticia altamente especializada con capacidades cibernéticas estratégicas avanzadas y conocimiento total de la situación.

DINÁMICO

El ministerio responsable de la defensa contribuye al debate mediante el desarrollo de un entendimiento internacional común del punto en el que un ataque cibernético podría desencadenar una respuesta de varios dominios.

Coordinación

INICIAL

Las fuerzas armadas nacionales no tienen capacidad, o tienen capacidad limitada, de resiliencia cibernética, destinada a reducir las vulnerabilidades de los intereses de seguridad nacional e infraestructura de red de defensa.

FORMATIVO

Se acuerdan los requisitos de capacidad de defensa cibernética entre el sector público y privado con el fin de minimizar la amenaza a la seguridad nacional.

ESTABLECIDO

Existe coordinación, en respuesta a los ataques maliciosos a los sistemas de información militar y a la infraestructura crítica nacional; existe un mecanismo para el intercambio de información que sirve para el análisis de amenazas y la recopilación de inteligencia.

ESTRATÉGICO

Existe cierta capacidad analítica para apoyar la coordinación y asignación de recursos para la defensa cibernética nacional, posiblemente incluyendo un centro de investigación de defensa cibernética.

DINÁMICO

La entidad encargada de la defensa cibernética coordina la integración estratégica con respecto a eventos cibernéticos entre el gobierno, los militares y la infraestructura crítica, incluidos los presupuestos, e identifica los roles y responsabilidades claras; este proceso luego alimenta a la re-evaluación de la situación de seguridad nacional del país.

Cultura y sociedad

Mentalidad de seguridad cibernética
En el gobierno
En el sector privado
En la sociedad

Conciencia de seguridad cibernética
Sensibilización

Confianza en el uso de Internet
En los servicios en línea
En el gobierno electrónico
En el comercio electrónico

Privacidad en línea
Normas de privacidad
Privacidad del empleado

Mentalidad de seguridad cibernética

Una mentalidad de seguridad cibernética incluye los valores, actitudes y prácticas, hábitos de usuarios individuales, expertos y otros actores en el ecosistema de la seguridad cibernética. Se les requiere a diferentes actores tener diversas mentalidades de seguridad cibernética, en función a sus roles y funciones en el ecosistema, incluyendo el gobierno, el sector privado, la academia, los expertos y el comportamiento responsable en línea. Los factores socioeconómicos contribuyen a la existencia de diferentes percepciones de la seguridad cibernética y pueden incidir en el hecho de que la misma se brinde de manera eficaz.

En el gobierno

INICIAL

No existe o se reconoce mínimamente una mentalidad de seguridad cibernética dentro de las agencias gubernamentales.

FORMATIVO

Agencias líderes han comenzado a darle prioridad a la seguridad cibernética, mediante la identificación de los riesgos y amenazas.

ESTABLECIDO

Mejores prácticas en seguridad cibernética son ampliamente conocidas en todo el gobierno en todos los niveles.

ESTRATÉGICO

La mayoría de las agencias en todos los niveles de gobierno han incorporado una mentalidad proactiva de seguridad cibernética, que sustenta la planeación estratégica.

DINÁMICO

La mentalidad de la seguridad cibernética es habitual e informa a todas las iniciativas relacionadas con la TI; la mentalidad de seguridad cibernética sirve como base para los enfoques individuales de los empleados ministeriales sobre sus responsabilidades.

En el sector privado

INICIAL

No existe o se reconoce mínimamente en la industria y los negocios la necesidad de darle prioridad a una mentalidad de seguridad cibernética.

FORMATIVO

Empresas líderes han comenzado a darle prioridad a una mentalidad de seguridad cibernética mediante la identificación de prácticas de alto riesgo.

ESTABLECIDO

Se ha arraigado una mentalidad de seguridad cibernética entre las empresas y la industria.

ESTRATÉGICO

Todas las organizaciones, incluidas las PYME, entre la mayoría de las industrias, han fomentado una mentalidad proactiva de seguridad cibernética, que informa a la planeación estratégica.

DINÁMICO

La mentalidad de seguridad cibernética sirve como base para los enfoques individuales dentro del sector privado respecto de las responsabilidades laborales e informa a todas las iniciativas relacionadas con TI.

En la sociedad

INICIAL

La sociedad desconoce las amenazas cibernéticas y no puede tomar medidas concretas de seguridad cibernética o la sociedad es consciente de las amenazas cibernéticas, pero no toma medidas proactivas para mejorar su seguridad cibernética.

FORMATIVO

Se adopta una mentalidad de seguridad cibernética, pero de manera inconsistente, en toda la sociedad; los programas y materiales han sido puestos a disposición para entrenar y mejorar las prácticas de seguridad cibernética.

ESTABLECIDO

Se ha desarrollado una conciencia social del uso seguro de los sistemas en línea; una proporción creciente de usuarios tienen las habilidades para manejar su privacidad en línea y protegerse de la intromisión, interferencia o acceso no deseado a la información por parte de otros.

ESTRATÉGICO

Un número creciente de usuarios están empleando prácticas seguras en línea como una costumbre, la conciencia de la seguridad está arraigada; la mayoría de los usuarios tienen la información, confianza y herramientas prácticas para protegerse en línea, mientras que se proporcionan el apoyo y los recursos a los miembros vulnerables de la sociedad, incluida la protección de menores.

DINÁMICO

Los usuarios demuestran una mentalidad de seguridad cibernética y emplean habitualmente las prácticas más seguras en su uso cotidiano de las redes en línea; el conjunto de habilidades en seguridad cibernética de la población de un país muestra un grado de desarrollo avanzado, por lo que los usuarios pueden abordar de manera efectiva las amenazas que enfrenta la sociedad.

Conciencia de seguridad cibernética

Sensibilización

Necesidad de que los programas aumenten la conciencia de seguridad cibernética con especial énfasis en la percepción de los riesgos y amenazas cibernéticas.

INICIAL

La necesidad de tomar conciencia de las amenazas y vulnerabilidades de seguridad cibernética en el sector público y privado no es reconocida o se encuentra en una fase inicial de discusión.

FORMATIVO

Se establecen campañas de sensibilización con objetivos definidos, pero son ad hoc, no cubren necesariamente todos los grupos y no están estrechamente vinculadas a la estrategia de seguridad cibernética; están disponibles seminarios y recursos en línea para la población objetivo, pero no hay esfuerzos de coordinación o de medición.

ESTABLECIDO

Existe un programa coordinado nacional para la concienciación sobre la seguridad cibernética en base a consultas con las partes interesadas, que se dirige a una amplia gama de grupos demográficos; se puede evidenciar la participación de múltiples partes interesadas en la prestación de servicios y productos de sensibilización.

ESTRATÉGICO

Se han establecido métricas para medir la eficacia de las campañas de sensibilización y los resultados sirven de base para campañas futuras, teniendo en cuenta brechas o fallas; el programa es apoyado por procesos para obtener medidas de idoneidad y calidad para la potencial reutilización del material; existe, es ampliamente conocido y fácilmente accesible un portal central en línea que tiene vínculos con información relevante.

DINÁMICO

Mediciones de rendimiento de las campañas de sensibilización sirven de base para los procesos nacionales de renovación de estrategias y la redistribución de los recursos; la comunidad de interesados aporta requisitos al proceso de planeación de la campaña, con un diseño específico para los grupos destinatarios.

Confianza en el uso de Internet

En los servicios en línea

El nivel de confianza de los individuos en el uso de Internet (servicios en línea y gobierno o comercio electrónico) determina la medida en que proporcionarán información personal en línea.

INICIAL

No existe o hay un uso mínimo de los servicios en línea; la confianza en los servicios en línea no es una preocupación; por lo tanto, los operadores de la infraestructura de Internet no han establecido acciones coordinadas.

FORMATIVO

La confianza en los servicios en línea se identifica como una preocupación; los operadores de infraestructuras toman en consideración medidas para fomentar la confianza en los servicios en línea; sin embargo, no se han establecido medidas.

ESTABLECIDO

Se han implementado esfuerzos para proporcionar servicios en línea más seguros; se ha establecido un programa nacional coordinado para promover la confianza en los servicios en línea; la asignación presupuestal para las medidas de seguridad para los servicios en línea es mínima.

ESTRATÉGICO

Se recogen las medidas de efectividad de un programa para promover la confianza incluyendo la consideración de los impactos secundarios y se utilizan para informar la asignación de recursos; las medidas que evalúan la confianza en los servicios en línea incluyen la sensación de control del individuo sobre el suministro de datos personales en línea.

DINÁMICO

A través de la aplicación y la evaluación iterativa de indicadores cuantitativos y cualitativos en la infraestructura en línea y la mejora en el desarrollo de servicios, aumenta la confianza en los servicios en línea; las personas evalúan el riesgo en el uso de servicios en línea y de forma continua ajustan su comportamiento sobre la base de esta evaluación.

En el gobierno electrónico

INICIAL

El gobierno no ofrece servicios electrónicos o los que ofrece son mínimos; si se ofrecen servicios electrónicos mínimos, el gobierno no ha promovido públicamente el entorno seguro necesario.

FORMATIVO

La gama de servicios electrónicos del gobierno continúa en expansión, con un reconocimiento de la necesidad de aplicar medidas de seguridad para promover la confianza en los servicios electrónicos; múltiples partes interesadas analizan las prácticas indeseables en línea.

ESTABLECIDO

Las infracciones se han identificado y reconocido y se dan a conocer de una manera ad hoc por el gobierno; el sector público coordina acciones para evitar ataques a la información personal; se priorizan los delitos en Internet de alto nivel; se promueve el cumplimiento de los estándares de Internet y de la web para proteger el anonimato de los usuarios.

ESTRATÉGICO

La divulgación de la información se hace por defecto; las preocupaciones sobre seguridad cibernética impulsan al gobierno; se promueve la privacidad por defecto como una herramienta para la transparencia; se emplean procesos de contenido generado por el usuario para proporcionar información sobre material ineficaz; se establecen medidas procesales para asegurar una gestión eficiente de los contenidos en línea.

DINÁMICO

Se mejoran continuamente los servicios de gobierno electrónico con el fin de promover un sistema transparente, abierto y seguro en el que la gente confía; se están llevando a cabo de manera consistente evaluaciones de impacto sobre la protección de la privacidad en las disposiciones de gobierno electrónico, las cuales retroalimentan la planeación estratégica.

En el comercio electrónico

INICIAL

No se ofrecen servicios de comercio electrónico; si se ofrecen, el entorno es inseguro y los usuarios carecen de un conocimiento adecuado de los servicios de comercio electrónico.

FORMATIVO

Los servicios de comercio electrónico son mínimos y no totalmente organizados; las partes interesadas y los usuarios reconocen la necesidad de seguridad en los servicios electrónicos y ha comenzado el análisis de inversión entre los proveedores de servicios.

ESTABLECIDO

Los servicios de comercio electrónico están plenamente establecidos en un entorno seguro; múltiples partes interesadas invierten en el comercio electrónico.

ESTRATÉGICO

Se han establecido la funcionalidad del servicio mejorado, la provisión de mecanismos de retroalimentación y la protección de la información personal para asegurar la continuidad del negocio.

DINÁMICO

Mediciones de desempeño continuas de servicios de comercio electrónico impulsan e informan la planeación estratégica; los términos y condiciones previstos en los servicios de comercio electrónico son claros y comprensibles para todos los usuarios.

Privacidad en línea

Las cuestiones de privacidad incluyen el intercambio de datos de carácter personal en el sector público y privado. Se aborda por separado el componente de protección de datos de la privacidad en las dimensiones 4 y 5. Los países con estrategias sofisticadas de seguridad cibernética no comprometerán la libertad de expresión en línea en nombre de la seguridad de la red.

Normas de privacidad

INICIAL

La discusión con grupos de interés sobre asuntos de privacidad ha comenzado a nivel gubernamental.

FORMATIVO

Se consideran las leyes y políticas que promueven el acceso a datos personales recogidos y almacenados por todo el gobierno y otras instituciones públicas.

ESTABLECIDO

Todos los actores relevantes de la sociedad civil están impulsando activamente el cambio en las prácticas, leyes y regulaciones que afectan la libertad de expresión en asuntos de privacidad; el gobierno está considerando la adopción de legislación sobre derechos humanos con un enfoque en la privacidad.

ESTRATÉGICO

Se adhiere a estándares de derechos humanos reconocidos a nivel regional e internacional, en relación a la privacidad.

DINÁMICO

Están claramente identificados los actores, políticas y prácticas que determinan la libertad de expresión y la privacidad y son fundamentales para informar las decisiones; se logra el cumplimiento de la declaración universal de los derechos humanos.

Privacidad del empleado

INICIAL

No hay debate, o es mínimo, entre los líderes del sector privado con respecto a las cuestiones de privacidad en el lugar de trabajo.

FORMATIVO

Se reconoce la privacidad en el lugar de trabajo como un componente importante de la seguridad cibernética y está empezando a ser institucionalizada en programas para empleados.

ESTABLECIDO

Los empleadores mantienen políticas de privacidad que ofrecen un nivel mínimo de privacidad para los empleados.

ESTRATÉGICO

Los empleados no solo toman conciencia de sus derechos a la privacidad dentro de la organización y se entienden las obligaciones de privacidad individual sobre la base de la planeación estratégica, sino que la organización también realiza auditorías externas para asegurar el cumplimiento de las normas de privacidad; se logra el cumplimiento de las mejores prácticas relacionadas con los derechos humanos sobre la privacidad en el lugar de trabajo y se evalúa a través de un proceso de auditoría.

DINÁMICO

Se llevan a cabo de manera regular evaluaciones de impacto sobre la privacidad, las cuales sustentan la revisión de la política.

Educación

Disponibilidad nacional de la educación y formación cibernéticas
Educación
Formación

Desarrollo nacional de la educación de seguridad cibernética
Desarrollo nacional de la educación de seguridad cibernética

Formación e iniciativas educativas públicas y privadas
Capacitación de empleados

Gobernanza corporativa, conocimiento y normas
En las empresas estatales y privadas

Disponibilidad nacional de la educación y formación cibernéticas

Recursos y/o financiación del país destinados a incrementar la disponibilidad de la educación y la formación en seguridad cibernética. Esta disponibilidad debe reflejar las necesidades en el ámbito activo de la seguridad cibernética.

Educación

INICIAL

No hay oferta educativa en seguridad de la información, o existe una oferta mínima pero no hay un proveedor reconocido de educación en seguridad cibernética; no existe una acreditación en educación en seguridad cibernética.

FORMATIVO

Existe mercado para la educación y la formación en seguridad de la información con evidencia de asimilación; las iniciativas de los profesionales están dirigidas a incrementar el atractivo de las carreras en seguridad cibernética y su pertinencia para roles de liderazgo más amplios.

ESTABLECIDO

Existen algunas ofertas educativas en seguridad cibernética a nivel nacional e institucional, que abarcan desde el nivel elemental hasta postgrado, incluyendo la formación profesional en forma modular.

ESTRATÉGICO

La oferta educativa se pondera y se centra sobre la base de una comprensión de los riesgos actuales y las necesidades de habilidades; se desarrollan métricas para asegurar que las inversiones educativas respondan a las necesidades del entorno de la seguridad cibernética; los educadores tienen acceso disponible en este campo, en particular los especialistas en seguridad cibernética.

DINÁMICO

Existe integración y sinergia entre los elementos educativos; los requisitos de seguridad cibernética que prevalecen son tomados en consideración en el re-desarrollo de todo programa general de estudios; la investigación y el desarrollo son una consideración principal en la educación sobre seguridad cibernética; el contenido de los programas de educación se alinea con desafíos operacionales y seguridad cibernética práctica.

Formación

INICIAL

No existe, o es mínima, la formación en seguridad cibernética.

FORMATIVO

Existe capacitación en seguridad de la información, pero es ad hoc y sin coordinación; en cuanto a formación, hay disponibles seminarios y recursos en línea para grupos demográficos específicos, pero no existen medidas de efectividad.

ESTABLECIDO

Los interesados invierten en capacitación en seguridad cibernética, lo cual no solo es aplicable a roles de TI sino también a roles ejecutivos, de gerencia y a toda una gama de empleados; se entienden bien las necesidades de la sociedad y están documentados los requisitos de formación; se evalúa la eficacia de los modos y procedimientos de formación y se establecen algunas métricas.

ESTRATÉGICO

Está disponible una variedad de cursos de capacitación en seguridad cibernética de alta calidad y estos son reconocidos internacionalmente; es clara la conexión de los programas de capacitación y educación con las prioridades de la estrategia nacional e institucional de seguridad cibernética.

DINÁMICO

Existe colaboración en la formación del sector público y privado, y la capacitación está disponible localmente y se adapta constantemente a los cambios del entorno ya que trata de construir conjuntos de habilidades en ambos sectores; existen incentivos patrocinados por los sectores público y privado para la formación.

Disponibilidad nacional de la educación y formación cibernéticas
Educación
- Formación

Desarrollo nacional de la educación de seguridad cibernética

Existencia de programas de educación en seguridad cibernética, títulos universitarios y de otro tipo de educación de alta calidad y cursos sobre seguridad cibernética. Creación de centros nacionales e internacionales cibernéticos de excelencia.

Desarrollo nacional de la educación de seguridad cibernética

INICIAL

No existen instructores profesionales en seguridad cibernética, o son pocos; no se cuenta con un programa para capacitar a instructores en seguridad cibernética; o no existe o apenas está siendo discutida la justificación del presupuesto para la educación y la investigación.

FORMATIVO

Existen incentivos para la formación y la educación; se identifican líneas presupuestales para la formación y la investigación y el desarrollo, con una oficina establecida para el desarrollo y ejecución del programa; se establece la participación de las partes interesadas para garantizar la continuidad.

ESTABLECIDO

Existen esfuerzos del sector privado y público para establecer programas para mejorar las competencias y la capacidad en materia de seguridad cibernética; una amplia consulta de múltiples partes interesadas informa las prioridades de la educación y de cualificaciones nacionales; socios académicos internacionales han sido consultados para beneficiarse de las lecciones aprendidas; existen centros de excelencia en seguridad cibernética financiados por el gobierno, accesibilidad a habilidades y educación cibernética, alineación de la educación con los problemas del mundo real y financiación dedicada a la investigación nacional.

ESTRATÉGICO

Se incrementa el presupuesto y el gasto del gobierno en capacitación y educación en seguridad cibernética sobre la base del rendimiento de la inversión; las iniciativas gubernamentales encaminadas a aumentar el atractivo de las carreras de seguridad cibernética se sustentan en un análisis de la brecha de las competencias existentes; se ha mejorado la cooperación y la colaboración entre las partes interesadas.

DINÁMICO

Existe disponibilidad de títulos universitarios y de otro tipo de educación de alta calidad y cursos sobre seguridad cibernética; los programas de educación en seguridad cibernética mantienen un equilibrio entre la conservación de los componentes básicos del currículo y la promoción de los procesos de adaptación que responden a cambios rápidos en el entorno de la seguridad cibernética; se establecen centros cibernéticos internacionales de excelencia a través de programas de hermanamiento dirigidos por instituciones de clase mundial.

Formación e iniciativas educativas públicas y privadas

Programas destinados a mejorar las habilidades de los empleados para que puedan enfrentar los problemas de seguridad cibernética a medida que ocurren.

Capacitación de empleados

INICIAL

No se llevan a cabo programas de capacitación en seguridad cibernética; poco personal de TI capacitado es designado para apoyar los problemas de seguridad cibernética a medida que se producen; puede haber conjuntos de habilidades, pero no se encuentran estratégicamente ubicados y las herramientas están limitadas a usuarios autorizados.

FORMATIVO

No hay transferencia de conocimientos por parte de los empleados de seguridad cibernética capacitados; debido a una formación limitada, solo hay uso informal de herramientas, modelos o plantillas existentes para la planeación de la seguridad cibernética de la organización, sin la integración automatizada de datos.

ESTABLECIDO

Existe transferencia de conocimientos de los empleados de seguridad cibernética formados, sobre una base ad hoc; se establecen iniciativas de creación de empleo para la seguridad cibernética y esto alienta a los empleadores a capacitar al personal; existen programas estructurados de capacitación en seguridad cibernética que especifican funciones y responsabilidades precisas; algunos sistemas de datos, herramientas y modelos están disponibles con personal capacitado limitado para operar; la formación técnica sigue siendo necesaria.

ESTRATÉGICO

Existe un cuadro suficientemente establecido de empleados cualificados formados en cuestiones, procesos, planeación y análisis de seguridad cibernética de la organización; el programa de desarrollo de habilidades de seguridad cibernética está integrado, optimizado y automatizado; los niveles de profesionalismo en seguridad de la información y seguridad cibernética son más evidentes en todo el sector público y privado.

DINÁMICO

Es continuo el intercambio de conocimientos de seguridad cibernética para promover el desarrollo de habilidades; se utiliza la gestión del ciclo de vida de la capacitación en seguridad cibernética para servir a futuros programas de capacitación; los sistemas de datos, herramientas y modelos son utilizados por una amplia gama de profesionales; ahora es posible la integración automatizada de datos, gracias a un grupo de habilidades avanzado en seguridad cibernética.

Gobernanza corporativa, conocimiento y normas

En las empresas estatales y privadas

Comprensión por parte de las juntas directivas de los riesgos que enfrentan las empresas, algunos de los principales métodos de ataque y cómo su empresa se ocupa de asuntos cibernéticos.

INICIAL

Las juntas directivas no consideran la seguridad cibernética, o lo hacen mínimamente; no se analizan consideraciones del deber fiduciario.

FORMATIVO

Las juntas directivas tienen algún conocimiento de cuestiones de seguridad cibernética, pero no de la forma en que estas podrían afectar a la organización, o cuáles serían las amenazas directas que pudieran enfrentar.

ESTABLECIDO

Las juntas directivas tienen una comprensión de la generalidad de cómo están en riesgo las empresas, algunos de los principales métodos de ataque y cómo su empresa se ocupa de cuestiones cibernéticas (cuestión que suele ser delegada al Director de Información); la gestión de eventos es en gran medida reactiva.

ESTRATÉGICO

Las juntas directivas conocen sus activos estratégicos, han puesto en marcha medidas específicas para protegerlos y conocen el mecanismo por medio del cual se protegen; la junta puede asignarles fondos y gente específica a los distintos elementos de riesgo cibernético, dependiendo de la situación que prevalece en su propia empresa; los planes de contingencia corporativos están listos para hacerles frente a diversos ataques cibernéticos y sus consecuencias; se proporciona algún tipo de formación obligatoria para la junta en seguridad cibernética; la junta tiene un claro sentido de los deberes fiduciarios cibernéticos.

DINÁMICO

Las juntas directivas pueden cambiar la estrategia de seguridad cibernética rápida y adecuadamente; se analizan las nuevas amenazas en cada reunión de junta y se reasigna la financiación y la atención para hacerles frente a esas amenazas; se acude a la junta como una fuente de conocimiento en gobernanza de seguridad cibernética corporativa; la gobernabilidad de la junta se basa en el riesgo cibernético y mejora la gobernabilidad específicamente en esta área.

Marcos legales

Marcos jurídicos de seguridad cibernética
Para la seguridad de las TIC
Privacidad, protección de datos y otros derechos humanos
Derecho sustantivo de delincuencia cibernética
Derecho procesal de delincuencia cibernética

Investigación jurídica
Cumplimiento de la ley
Fiscalía
Tribunales

Divulgación responsable de la información
Divulgación responsable de la información

Marcos jurídicos de seguridad cibernética

Incluye los marcos jurídicos sobre las TIC, la privacidad, los derechos humanos y la protección de datos y el derecho sustantivo y procesal de delincuencia cibernética, y todos incluyen cooperación internacional.

Para la seguridad de las TIC

INICIAL

La legislación relativa a la seguridad de las TIC aún no existe o está en proceso de desarrollo; si está en proceso, se han hecho los esfuerzos para llamar la atención sobre la necesidad de crear un marco jurídico sobre la seguridad cibernética y puede incluirse la necesidad de un análisis de deficiencias.

FORMATIVO

Los socios experimentados han sido consultados para apoyar el establecimiento de marcos jurídicos y reglamentarios; se han identificado prioridades clave para la creación de marcos legales de seguridad cibernética, pero aún no se han establecido a través de una consulta público-privada y con múltiples partes interesadas.

ESTABLECIDO

Se han implementado los marcos legislativos y reglamentarios de seguridad integral de las TIC que abordan la seguridad cibernética; se ha adoptado la legislación que protege los derechos de los individuos y las organizaciones en el entorno digital.

ESTRATÉGICO

Las leyes vigentes y los mecanismos de regulación han sido revisados, identificando dónde existen brechas y solapamientos; se priorizan aquellas áreas que necesitan mejoras; se garantiza la integridad, confidencialidad, disponibilidad y seguridad global de la información digital y las TIC a través de la revisión periódica y mejora de las medidas legales y reglamentarias.

DINÁMICO

Se establecen mecanismos para optimizar el sector de la seguridad TIC a través de enmiendas o promulgación de legislación y de la mejora de la armonización de los marcos legales de las TIC con otras políticas, leyes, normas y mejores prácticas; existen medidas para contribuir al desarrollo de mejores prácticas internacionales que informarán al marco normativo nacional.

Privacidad, protección de datos y otros derechos humanos

INICIAL

No existe legislación de privacidad y protección de datos o está en proceso de desarrollo; la legislación nacional no reconoce los derechos humanos y civiles fundamentales en relación con delitos relacionados con la cibernética.

FORMATIVO

Existe legislación parcial respecto a la privacidad, protección de datos y libertad de expresión.

ESTABLECIDO

Se han aplicado procedimientos reglamentarios y legislación de protección de datos integral; la legislación nacional prevé el derecho del individuo a la privacidad especificando el aviso, el propósito, el consentimiento, la seguridad, la divulgación, el acceso y la responsabilidad de la información personal.

ESTRATÉGICO

Se ha adoptado una estructura integral del sistema de justicia penal para luchar contra los delitos relacionados con la cibernética, respetando los derechos humanos; el país está comprometido y trabaja con organizaciones internacionales sobre protección de datos y privacidad.

DINÁMICO

El país ha adoptado una legislación adecuada, que incluye aquella encaminada al fomento de la cooperación internacional y la asistencia judicial recíproca con el fin de combatir los delitos contra la protección de datos y privacidad, al facilitar su detección, investigación y judicialización tanto a nivel nacional como internacional. Si procede, ha ratificado o se ha adherido a los tratados y otros acuerdos internacionales de protección de datos.

Derecho sustantivo de delincuencia cibernética

INICIAL

El derecho penal sustantivo específico para la delincuencia cibernética no existe, o existe el derecho penal general y se aplica ad hoc a la delincuencia cibernética.

FORMATIVO

Existe una legislación parcial en el derecho penal sustantivo que aplica los marcos legales y regulatorios a algunos aspectos de los delitos cibernéticos; está siendo discutido el derecho penal sustantivo para la delincuencia cibernética entre los legisladores, pero ha comenzado el desarrollo de la ley.

ESTABLECIDO

La legislación vigente tipifica una serie de delitos relacionados con pruebas electrónicas que pueden ser objeto de una legislación específica o abordados en el código penal.

ESTRATÉGICO

El país se adhiere a las mejores prácticas y normativas regionales e internacionales pertinentes sobre derecho de delito cibernético y asigna los recursos de acuerdo a las prioridades nacionales.

DINÁMICO

El país continuamente busca incluir el desarrollo de las mejores prácticas internacionales sobre delito cibernético en la legislación nacional y es un colaborador activo en el discurso global sobre la mejora de los instrumentos de la lucha contra delitos cibernéticos internacionales; existen medidas para superar en el país las líneas de base mínimas de seguridad internacional.

Derecho procesal de delincuencia cibernética

INICIAL

No existe el derecho penal procesal adecuado para la delincuencia cibernética y el uso de la prueba electrónica en otros crímenes, o existe el derecho penal procesal general y se aplica ad hoc a la delincuencia cibernética y al uso de la prueba electrónica en otros crímenes.

FORMATIVO

Se está discutiendo y desarrollando el derecho procesal penal en relación con la prueba electrónica; el derecho procesal penal se aplica ad hoc a la delincuencia cibernética, pero no ha comenzado el desarrollo de los delitos cibernéticos específicos.

ESTABLECIDO

Se ha implementado el derecho procesal penal integral y los requisitos probatorios relacionados; las mejores prácticas se emplean por aplicación de la ley en el ejercicio de poderes procesales.

ESTRATÉGICO

En el caso de la investigación transfronteriza, el derecho procesal estipula las acciones que es necesario realizar bajo las características de casos particulares, con el fin de obtener con éxito la prueba electrónica.

DINÁMICO

El país se adhiere a las mejores prácticas internacionales sobre procedimiento penal de delito cibernético y la obtención de pruebas electrónicas, y constantemente busca implementar estas medidas en la legislación nacional y sirve como un colaborador activo en el discurso global sobre la mejora de la lucha contra los delitos cibernéticos internacionales; existen medidas para superar las líneas de base mínimas de seguridad internacional, que contribuyen al desarrollo de mejores prácticas internacionales.

Investigación jurídica

Capacidad de investigación para procesar las pruebas electrónicas y luchar contra la delincuencia cibernética, incluida la forma de evaluar, obtener y tratar la evidencia digital y utilizar los instrumentos procesales adecuados.

Cumplimiento de la ley

INICIAL

No existe la capacidad de las autoridades policiales para prevenir y combatir los delitos relacionados con la cibernética.

FORMATIVO

Existe alguna capacidad de investigación para indagar delitos que involucren pruebas electrónicas, así como para obtener dichas pruebas, de conformidad con el derecho interno; sin embargo, esta capacidad es mínima.

ESTABLECIDO

Se ha establecido una capacidad institucional integral para investigar y manejar casos de delincuencia cibernética y delitos relacionados con pruebas electrónicas, incluyendo los recursos humanos, procesales y tecnológicos, medidas exhaustivas de investigación, cadena de custodia digital y gestión de integridad de las pruebas y mecanismos formales e informales de colaboración con interesados internacionales y nacionales (actores de los sectores privado y público).

ESTRATÉGICO

Los oficiales de las fuerzas de la ley reciben una formación continua basada en las responsabilidades relativas y en entornos de amenazas nuevas y cambiantes y pueden utilizar herramientas forenses digitales sofisticadas para investigar delitos informáticos complejos y delitos relacionados con pruebas electrónicas; los organismos locales de aplicación de la ley colaboran con contrapartes regionales e internacionales en investigaciones.

DINÁMICO

Existen recursos dedicados a unidades de delitos informáticos plenamente operativas, incluyendo capacidades avanzadas de investigación y de gestión de integridad de los datos; es posible recoger y analizar las estadísticas y tendencias que mejorarían la investigación sobre los delincuentes con el fin de facilitar una comprensión exhaustiva del ambiente delictivo en línea y contribuir a la toma de decisiones estratégicas; las agencias de aplicación de la ley nacionales están participando plenamente en la investigación y redes transfronterizas.

Fiscalía

INICIAL

Los fiscales no están entrenados adecuadamente y no tienen la capacidad para enjuiciar los delitos relacionados con la informática; no existen recursos para comprender o revisar las pruebas electrónicas.

FORMATIVO

Un número limitado de fiscales tienen la capacidad de construir un caso basado en información electrónica, pero esta capacidad es en gran medida ad hoc, no institucionalizada, y se carece de mecanismos formales de colaboración con la policía.

ESTABLECIDO

Se ha establecido la capacidad institucional para procesar y manejar los casos de delitos cibernéticos y casos relacionados con pruebas electrónicas; existen suficientes recursos tecnológicos y capacitación en recursos humanos.

ESTRATÉGICO

Existen estructuras institucionales en operación que permiten una clara distribución de tareas y obligaciones dentro de la fiscalía en todos los niveles del gobierno; existe una relación estratégica entre los organismos policiales y la fiscalía, lo que permite que los procedimientos judiciales sean rápidos y precisos; se analizan mediciones, estadísticas y tendencias relacionadas con tasas de condenas exitosas.

DINÁMICO

Los fiscales tienen la capacidad de enjuiciar con éxito los delitos cibernéticos complejos en el país y realizar una colaboración transfronteriza; la formación está institucionalizada y es dinámica, teniendo en cuenta los entornos nuevos y cambiantes de amenazas.

Tribunales

INICIAL

Los jueces no aplican las pruebas electrónicas integralmente.

FORMATIVO

Un número limitado de jueces tiene capacidad para presidir un caso de delito cibernético, pero esta capacidad es en gran medida ad hoc y no sistemática; no existen recursos judiciales o de formación en delincuencia cibernética.

ESTABLECIDO

Están disponibles los recursos judiciales y se cuenta con capacitación suficiente para garantizar la judicialización eficaz y eficiente de casos de pruebas electrónicas y delincuencia cibernética.

ESTRATÉGICO

Se ha organizado el sistema judicial para garantizar una relación estratégica entre el Poder Judicial y la fiscalía, lo que permite que se adelanten procedimientos judiciales rápidos y precisos; se encuentran en funcionamiento mecanismos de cooperación para asegurar la ejecución de órdenes extraterritoriales.

DINÁMICO

El Poder Judicial recibe formación continua basada en las responsabilidades relativas y en los entornos cambiantes de amenazas; el sistema judicial está al tanto de los constantes cambios en el entorno de la seguridad cibernética y asigna recursos cuando corresponde.

Divulgación responsable de la información

Una divulgación responsable vigente puede proporcionar directrices y declaraciones específicas que abordan cómo se revelará una vulnerabilidad y puede mejorar la capacidad de seguridad mediante la reparación de la vulnerabilidad y la prevención de cualquier daño futuro.

Este factor se refiere a un modelo de divulgación de vulnerabilidades o metodología de informes en que una parte (el informador) da a conocer de forma privada la información relacionada con una vulnerabilidad descubierta a un proveedor de producto o proveedor de servicios (parte afectada) y le otorga tiempo a la parte afectada para investigar la reclamación e identificar y probar un remedio o recurso antes de coordinar la divulgación pública de la vulnerabilidad con el informador.

Divulgación responsable de la información

INICIAL

No se reconoce la necesidad de una política de divulgación responsable en las organizaciones del sector público y privado.

FORMATIVO

Está vigente un marco de divulgación de vulnerabilidades, lo que incluye un plazo de divulgación, una resolución prevista y un informe de reconocimiento; se demuestra cierta capacidad de compartir detalles técnicos de la vulnerabilidad con otras partes interesadas que pueden distribuir la información de manera más amplia, a través de mayor cooperación público-privada.

ESTABLECIDO

Las organizaciones han desarrollado la capacidad de recibir y difundir información sobre la vulnerabilidad; proveedores de servicios y de software aceptan los informes de error y de vulnerabilidad y los abordan y se comprometen informalmente a abstenerse de adelantar acciones legales en contra de una parte que revela información responsablemente.

ESTRATÉGICO

Se publica un análisis de los detalles técnicos de la vulnerabilidad y se difunde información de asesoramiento de acuerdo a las funciones y responsabilidades; se establecen procesos de divulgación responsable de vulnerabilidades, incluidos los plazos para todos los interesados implicados (proveedores de productos, clientes, proveedores de seguridad y público); puede haber regulaciones para ordenar reportes de vulnerabilidades por parte de los operadores y propietarios de infraestructuras críticas.

DINÁMICO

Las políticas de divulgación responsable son revisadas y actualizadas de forma continua en base a las necesidades de los grupos de interés afectados; los mecanismos de divulgación responsable se sincronizan a nivel internacional; los procesos nacionales e internacionales para la revisión y la reducción de los plazos se encuentran en operación.

Tecnologías

Adhesión a las normas
Aplicación de las normas y prácticas mínimas aceptables
Adquisiciones
Desarrollo de software

Organizaciones de coordinación de seguridad cibernética
Centro de mando y control
Capacidad de respuesta a incidentes

Respuesta a incidentes
Identificación y designación
Organización
Coordinación

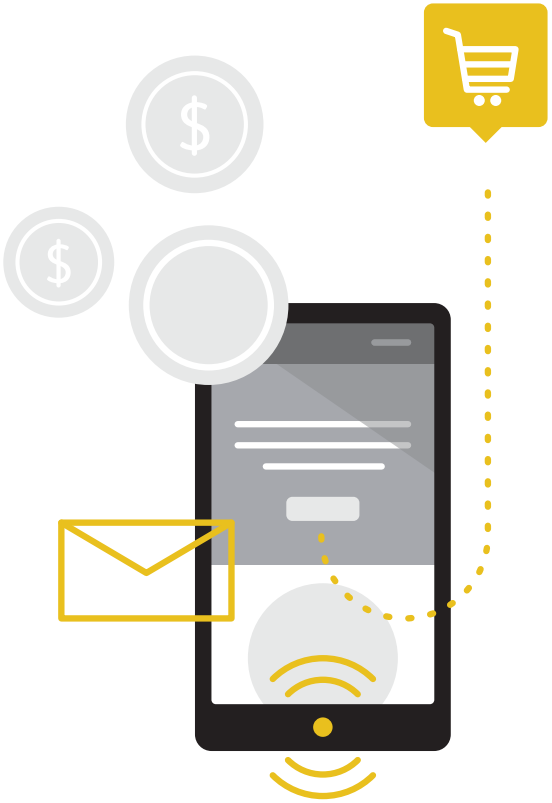
Resiliencia de la infraestructura nacional
Infraestructura tecnológica
Resiliencia nacional

Protección de la Infraestructura Crítica Nacional (ICN)
Identificación
Organización
Planeación de respuesta
Coordinación
Gestión de riesgos

Gestión de crisis
Planeación
Evaluación

Redundancia digital
Planeación
Organización

Mercado de la ciberseguridad
Tecnologías de seguridad cibernética
Seguros de delincuencia cibernética



Adhesión a las normas

Este factor se centra en la tecnología de infraestructura y la resiliencia de infraestructura nacional. La tecnología de infraestructura apuntala la vida cotidiana y asegura que el país siga funcionando social y económicamente. El gobierno y el sector privado son capaces de proteger los sistemas de información del país y los operadores de infraestructuras críticas para garantizar una mejor capacidad de recuperación nacional.

Aplicación de las normas y prácticas mínimas aceptables

INICIAL

O bien no se han identificado normas o prácticas para la seguridad de la información o la identificación es ad hoc y se carece de un esfuerzo concertado para aplicar esas normas.

FORMATIVO

Se han identificado estándares de seguridad de la información para su uso y ha habido algunos signos iniciales de promoción y adopción del gobierno, sector público y organizaciones de la Infraestructura Crítica Nacional (ICN); hay una aplicación mínima de las normas nacionales e internacionales.

ESTABLECIDO

Se ha identificado la línea de base acordada a nivel nacional de las normas relacionadas con la seguridad cibernética y prácticas menos aceptables y se han adoptado ampliamente en todo el sector público y las organizaciones del CNI; se mide y se reporta la adopción y cumplimiento, con supervisión de la adopción por parte del gobierno; se considera el uso de normas para mitigar el riesgo de los sistemas de abastecimiento de la ICN.

ESTRATÉGICO

Las normas se adoptan en el contexto de las decisiones presupuestarias y se asignan los recursos de acuerdo con las evaluaciones de riesgo y el debate entre los sectores público y privado, al igual que otras partes interesadas; se están desarrollando e implementando normas específicas del sector; existe evidencia de la contribución a los organismos de normalización internacionales y liderazgo de pensamiento e intercambio de experiencias de las organizaciones.

DINÁMICO

La mejora de procesos continua se aplica a la elección de las normas y métodos empleados y promueve la aplicación fluida; existe evidencia de la gestión de riesgos en colaboración en las decisiones relativas al incumplimiento por todos los sectores y ICN, adaptándose al panorama cambiante de la seguridad cibernética; existe evidencia de un debate maduro en la industria y la sociedad en general sobre el uso dinámico de las normas y prácticas basadas en la evaluación continua de necesidades.

Adquisiciones

INICIAL

No hay evidencia de uso de las normas relacionadas con la seguridad cibernética en la orientación de los procesos de adquisición, o existe algún reconocimiento de la orientación disponible, pero no existe ningún esfuerzo para utilizarlo.

FORMATIVO

Se están desarrollando normas de seguridad cibernética en las prácticas y procedimientos de contratación.

ESTABLECIDO

La aplicación de normas en las prácticas de contratación cumple con las directrices internacionales, las normas y las prácticas aceptables de TI y se evidencia a través de evaluaciones de medición y calidad de la efectividad del proceso.

ESTRATÉGICO

Aspectos críticos de adquisiciones y suministros, tales como precios y costos, calidad, plazos y otras actividades de valor agregado, se mejoran continuamente en el contexto de una planeación de recursos más amplios por todas las empresas; las habilidades de los profesionales de las adquisiciones pueden ser comparadas y evaluadas según las competencias señaladas en las normas de contratación pública; los grupos de interés internos tienen una comprensión global de los sistemas de compras electrónicas (e-sourcing) o licitaciones electrónicas (e-tendering) y el proceso integral de compras (P2P) con el fin de aplicar estas herramientas en la realización de las tareas clave en la contratación y suministro.

DINÁMICO

Las organizaciones tienen la capacidad de controlar el uso de las normas en los procesos de adquisiciones y apoyar las desviaciones y decisiones relativas al incumplimiento en tiempo real a través de la toma de decisiones basada en el riesgo; las mejores prácticas se incluyen en la contratación y cumplimiento de la garantía de calidad de las sociedades.

Desarrollo de software

INICIAL

No hay identificación de las normas de desarrollo de software en los sectores público y privado, o hay alguna identificación pero solo hay una evidencia limitada de asimilación.

FORMATIVO

Se están discutiendo metodologías para los procesos de desarrollo de software que se centran en la integridad y la capacidad de recuperación, y el gobierno y las comunidades profesionales las están promoviendo; existe evidencia de que dentro de la ICN y del sector público hay organizaciones que suministran y buscan adoptar normas de desarrollo de código y del logro de algunas acreditaciones con la promoción gubernamental de prácticas seguras.

ESTABLECIDO

El gobierno tiene un programa establecido para promover la adopción de estándares en el desarrollo de software, tanto para los sistemas del sector público como del sector privado, lo que incluye el seguimiento de la observancia de las normas; están presentes los sistemas de alta integridad y técnicas de desarrollo de software dentro de la oferta educativa y de formación.

ESTRATÉGICO

Se están incorporando consideraciones de seguridad cibernética en todas las etapas de desarrollo y procesos; se han adoptado las actividades básicas de desarrollo, incluyendo la configuración y gestión de documentos, desarrollo de la seguridad y la planeación del ciclo de vida del software; se realiza la selección de las normas, de los recursos y la toma de decisiones a través de la evaluación de riesgos.

DINÁMICO

Los proyectos de desarrollo de software evalúan continuamente el valor de las normas y reducen o mejoran los niveles de cumplimiento de acuerdo con decisiones basadas en el riesgo; los requisitos de seguridad cibernética están integrados en el ciclo de vida de las adquisiciones (requisitos de las necesidades, solicitudes de ofertas y contrato); en el caso del software estatal, se realizan las evaluaciones a lo largo de toda la vida del contrato.

Organizaciones de coordinación de seguridad cibernética

Este factor analiza la existencia y la actividad de los Equipos de Respuesta ante Incidentes de Seguridad Informática (CSIRT, por sus siglas en inglés) y el Centro de Mando y Control en el ámbito nacional, en términos de capacidad de respuesta ante incidentes y mitigación de las amenazas.

Centro de mando y control

INICIAL

No existe un centro de mando y control de la seguridad cibenética, o se está considerando crearlo a nivel nacional.

FORMATIVO

La función de mando y control está en manos, de manera informal, de la capacidad nacional de respuesta a incidentes o alguna otra entidad, sin una autoridad formal de coordinación.

ESTABLECIDO

Se identifica y existe una organización de mando y control, pero sin que haya recolección, procesamiento ni análisis automatizados; existe un mando y control ejecutivo oficial para el ciberespacio como un asunto estratégico nacional; se cuenta con una visión general de las capacidades de seguridad actuales, pero sin conocimiento de la situación.

ESTRATÉGICO

Se ha establecido un centro de mando y control con automatización mejorada, proporcionando un conocimiento básico de la situación nacional; se hace la selección de objetivos del centro de mando y control como parte de la planeación de recursos y el desarrollo de políticas estratégicas.

DINÁMICO

Hay un centro de mando y control de ciberespacio nacional completamente desarrollado, que recibe y correlaciona la información de las organizaciones con la capacidad de respuesta a incidentes, organizaciones públicas/privadas, los LSP (“Layered Service Providers” en inglés), la infraestructura crítica de la información, organizaciones de defensa e inteligencia, y que está altamente automatizado, lo que proporciona conocimiento avanzado de la situación; el conocimiento de la situación activa está coordinado con la oficina ejecutiva nacional.

Capacidad de respuesta a incidentes

INICIAL

La capacidad de respuesta de incidentes no es coordinada y se lleva a cabo de manera ad hoc.

FORMATIVO

Existe un equipo o personal de respuesta a incidentes en el país, con roles y responsabilidades identificadas; la actividad se concentra en la detección y respuesta a incidentes cibernéticos específicos de la organización.

ESTABLECIDO

Se ha establecido una capacidad de respuesta a incidentes nacional que involucra a los interesados clave, en especial a través de asociaciones público-privadas; la sostenibilidad financiera de la capacidad de respuesta a incidentes es considerada y planificada a través de la participación de las principales partes interesadas; se desarrolla e implementa un plan de gestión de vulnerabilidades; los incidentes se clasifican en consonancia con los planes de respuesta; los planes de respuesta y recuperación están operando y se gestionan; existe una evaluación nacional de la base de datos de vulnerabilidad del impacto en las funciones críticas; la información se comparte en consonancia con los planes de respuesta; los principales interesados son conscientes de la capacidad nacional de respuesta a incidentes y sus responsabilidades.

ESTRATÉGICO

La capacidad nacional de respuesta a incidentes apoya la creación de capacidades específicas del sector; se comparten los recursos y la información a través de una mayor coordinación y colaboración con los equipos locales, regionales e internacionales de respuesta a incidentes; la evaluación de la eficacia del CSIRT informa la dotación de recursos de este; los informes de incidentes ocurren en todos los sectores y planes de respuesta, y se ponen a prueba los correspondientes planes de recuperación; se ofrecen servicios forenses; el intercambio de información se promueve de manera voluntaria entre las partes interesadas externas.

DINÁMICO

La capacidad nacional de respuesta a incidentes es completamente sostenible financieramente y recibe apoyo político, independientemente de las transiciones políticas; existe una cooperación internacional orientada a la formación de mejores prácticas entre los grupos de expertos.

Respuesta a incidentes

No todos los incidentes cibernéticos pueden ser mitigados, por lo que la identificación de cuáles de estos eventos constituyen amenazas a nivel nacional puede ayudar a limitar el alcance de la responsabilidad. Además, un enfoque organizado y coordinado de respuesta a incidentes asegura que las amenazas puedan ser manejadas de la manera más eficiente posible.

Identificación y designación

INICIAL

No se identifican ni catalogan incidentes a nivel nacional.

FORMATIVO

Se han clasificado ciertos eventos cibernéticos o amenazas y se han registrado como incidentes o desafíos a nivel nacional.

ESTABLECIDO

Se establece un registro central de incidentes cibernéticos a nivel nacional.

ESTRATÉGICO

Se hacen y se priorizan actualizaciones regulares y sistemáticas en el registro de incidentes a nivel nacional; existe cierta capacidad para enfocar los recursos analíticos de respuesta a incidentes.

DINÁMICO

La capacidad para adaptar el enfoque en la identificación y análisis de incidentes es dinámica en respuesta a los cambios del entorno y puede incluir consideraciones de defensa cibernética.

Organización

INICIAL

La respuesta a incidentes a nivel nacional es limitada o inexistente; la respuesta, si la hay, es reactiva y ad hoc.

FORMATIVO

Han sido identificadas y contactadas las organizaciones del sector privado que son clave para la seguridad cibernética nacional, sin que haya mecanismos de coordinación o de intercambio de información con el sector público formal; un cuerpo central ha sido designado para recopilar información sobre amenazas de emergencia, sin un mandato específico para una agencia de respuesta cibernética nacional.

ESTABLECIDO

Existe una relación de coordinación rutinaria entre los sectores público y privado para responder a incidentes a nivel nacional con alcance limitado, pero la respuesta sigue siendo reactiva; se establece la capacidad de respuesta y la financiación para la función básica ha sido identificada.

ESTRATÉGICO

Se han establecido de manera clara y formal los roles y responsabilidades de seguridad cibernética para el gobierno, la infraestructura crítica, la empresa y los sistemas individuales; los recursos asignados a la respuesta de emergencia son adecuados para enfrentar el entorno de amenazas de seguridad cibernética.

DINÁMICO

Una capacidad de alerta temprana se incorpora a la misión de la organización de respuesta a emergencias, que busca darle forma a y/o gestionar el panorama de las amenazas antes de responder a desafíos específicos; las herramientas para la detección, identificación, prevención, respuesta y mitigación tempranas de vulnerabilidades de día cero están incluidas en la (s) organización (es) de respuesta a emergencias.

Coordinación

INICIAL

La responsabilidad de la respuesta a incidentes puede haber sido asignada, o no, de manera informal a un miembro del personal dentro de cada agencia y ministerio del gobierno.

FORMATIVO

Se han identificado y publicitado directores de incidentes en cada agencia y ministerio a nivel nacional; los canales de comunicación entre estos directores siguen siendo ad hoc e incoherentes.

ESTABLECIDO

Se ha establecido y publicado una respuesta nacional a incidentes coordinada, con procesos claros y funciones y responsabilidades definidas; se preparan líneas de comunicación para situaciones de crisis.

ESTRATÉGICO

Ahora las capacidades técnicas van más allá de la coordinación de la respuesta e incluyen análisis de incidentes y apoyo; se establecen servicios proactivos y servicios de gestión de calidad de la seguridad en las organizaciones subnacionales y sectoriales.

DINÁMICO

La respuesta a incidentes se adapta al entorno de amenazas; la coordinación nacional de varios niveles entre todos los niveles y sectores es fundamental para la respuesta a incidentes; existe coordinación entre las organizaciones regionales e internacionales de respuesta a incidentes.

Resiliencia de la infraestructura nacional

Este factor se enfoca en la tecnología de la infraestructura y la resiliencia de la infraestructura nacional. La tecnología de la infraestructura sustenta la vida cotidiana y asegura que el país siga funcionando social y económicamente. El gobierno y el sector privado pueden proteger los sistemas de información del país y los operadores de infraestructuras críticas para asegurar una mejor capacidad de recuperación nacional.

Infraestructura tecnológica

INICIAL

La infraestructura de servicios de Internet no es fiable; cuando es confiable los servicios son asequibles, pero con escasa utilización de las tarifas de servicios; la disponibilidad de la tecnología para apoyar el comercio electrónico y la interacción de negocio a negocio es una preocupación, pero no se ha establecido ninguna o casi ninguna acción coherente.

FORMATIVO

Se realiza el despliegue no estratégico de la tecnología y los procesos en los sectores público y privado; están disponibles en línea servicios públicos, información y contenidos digitales, pero son limitadas la implementación y el proceso.

ESTABLECIDO

Los procesos y tecnología desplegados cumplen estándares internacionales, directrices y mejores prácticas de TI; el uso de Internet para la comunicación entre todas las partes interesadas se integra en la práctica cotidiana de funcionamiento; el Internet se utiliza para el negocio de comercio electrónico y se establecen medidas y procesos de autenticación y transacciones electrónicas.

ESTRATÉGICO

Se han establecido procesos de seguridad rigurosos en los sectores privados y gubernamentales, especialmente para la gestión de riesgos de seguridad, evaluación de amenazas, respuesta a incidentes y la continuidad del negocio; se lleva a cabo una evaluación periódica de procesos y seguridad de la infraestructura de información nacional de acuerdo con las normas y directrices; se evalúan los beneficios medibles para las empresas de inversiones adicionales en tecnología.

DINÁMICO

Se controla con eficacia la adquisición de tecnologías de infraestructura, con una flexibilidad incorporada de acuerdo a los cambios en la dinámica del mercado; se evalúan y minimizan continuamente los costos de las tecnologías de infraestructura; los procesos están totalmente automatizados, y a menudo incorporados en la propia tecnología.

Resiliencia nacional

El gobierno no tiene control de la infraestructura tecnológica o este control es mínimo; las redes y sistemas son tercerizados, con potencial de adopción por parte de mercados de terceros poco fiables; puede haber una dependencia de otros países en tecnología de la seguridad cibernética.

FORMATIVO

La infraestructura nacional se gestiona de manera informal, sin procesos, funciones ni responsabilidades documentados; hay un apoyo regional para la tecnología de la seguridad cibernética y la infraestructura en el país.

ESTABLECIDO

La infraestructura nacional es administrada formalmente, con procesos, funciones y responsabilidades documentados y limitada redundancia; el apoyo regional a las tecnologías cibernéticas se complementa con un programa nacional para el desarrollo de infraestructura.

ESTRATÉGICO

Se lleva a cabo la gestión basada en los riesgos y las mejores prácticas con el análisis formal de las vulnerabilidades; se llevan a cabo evaluaciones de la capacidad de recuperación nacional para la ICN y los servicios esenciales para proteger los sistemas de información del país y los operadores de ICN y los servicios esenciales.

DINÁMICO

La adquisición de tecnologías críticas está controlada eficazmente, con una gestión de los procesos de continuidad de servicio y de la planeación estratégica; es predominante la alta disponibilidad de tecnologías críticas como parte del marco de gobernanza formal; se mantienen, mejoran y perpetúan sistemáticamente las capacidades científicas, técnicas, industriales y humanas con el fin de mantener la resiliencia independiente del país.

Resiliencia de la infraestructura nacional
Infraestructura tecnológica
• Resiliencia nacional

Protección de la Infraestructura Crítica Nacional (ICN)

Si bien los distintos gobiernos pueden identificar diferentes entidades como "infraestructura crítica", es importante que se tomen las medidas adecuadas para proporcionar la seguridad cibernética necesaria para proteger estos activos cruciales. Estas medidas deben basarse en una cuidadosa planeación y gestión adecuada del riesgo.

Identificación

INICIAL

Se entiende poco o nada de los activos y las vulnerabilidades de la ICN, pero no han sido identificadas las vulnerabilidades o categorización formal.

FORMATIVO

Se ha creado una lista general de activos de la ICN, sin identificar prioridades basadas en el riesgo.

ESTABLECIDO

Se lleva a cabo una auditoría de los activos de la ICN de forma regular; se analiza con las partes interesadas la difusión de las listas de auditoría de activos de la ICN en función de un modelo de asociación público-privada.

ESTRATÉGICO

Los riesgos de la ICN han sido priorizados de acuerdo a la vulnerabilidad y el impacto, lo que guía las inversiones estratégicas; se han determinado y establecido los procesos de gestión de activos y de vulnerabilidad de los activos de la ICN para que se puedan hacer las mejoras continuas de seguridad; se ha hecho una distinción entre los activos de la ICN y servicios esenciales para la actividad del día a día.

DINÁMICO

La lista de prioridades de los activos de la ICN se re-evalúa regularmente para capturar los cambios en el entorno de amenazas; se entiende y se incorpora a la planeación futura el impacto del riesgo de la seguridad cibernética en las operaciones comerciales de los propietarios de los activos de la ICN, incluyendo los costos directos y de oportunidad, el impacto en los ingresos y los obstáculos a la innovación.

Organización

INICIAL

Hay poca o ninguna interacción entre los ministerios gubernamentales y los propietarios de los activos críticos; no existe un mecanismo de colaboración formal.

FORMATIVO

Se establece un mecanismo para la divulgación periódica de vulnerabilidades entre el sector público y privado, pero no se ha especificado el alcance de los requisitos de presentación de informes.

ESTABLECIDO

Los requisitos de información definidos entre los propietarios de activos de la ICN y el sector público son suficientes para atender las necesidades de seguridad nacional.

ESTRATÉGICO

Existe un claro entendimiento de las responsabilidades y obligaciones de los propietarios y operadores de los activos de la ICN; se observa cooperación y coordinación con los ministerios y las agencias nacionales de seguridad.

DINÁMICO

En la regulación de los activos del ICN, se logró un equilibrio entre la satisfacción de las necesidades nacionales de seguridad cibernética y la implicación de costos.

Planeación de respuesta

INICIAL

La planeación de la respuesta a un ataque a los activos críticos puede haber sido discutida ampliamente, pero no existe un plan formal.

FORMATIVO

La protección de los activos críticos incluye las políticas de seguridad de datos y sensibilización sobre seguridad cibernética a nivel básico pero no se han acordado procesos o procedimientos de protección.

ESTABLECIDO

Se han establecido procedimientos y procesos de protección de información con el apoyo de soluciones de seguridad técnicas adecuadas; se utilizan procedimientos de gestión de riesgos para crear un plan de respuesta y producir un curso repetible de actuación en caso de incidentes; se comprueban los enlaces de comunicación, se llevan a cabo medidas de mitigación de daños y análisis y se realizan ejercicios para prepararse para un evento.

ESTRATÉGICO

Se lleva a cabo con regularidad la evaluación de la gravedad de un incidente en activos críticos y la planeación de la respuesta se basa en esa evaluación; las mejoras en los mecanismos de respuesta se llevan a cabo rutinariamente a fin de promover respuestas estratégicas.

DINÁMICO

La supervisión continua de la seguridad garantiza que las medidas de protección demuestren la eficacia continua e indica qué tecnologías, políticas o procesos requieren cambios; se ha establecido un mercado de seguros para la seguridad cibernética y se han explorado opciones para el reaseguro para apoyar la continuidad del negocio.

Coordinación

INICIAL

Los procedimientos informales de diálogo entre el sector público y privado son inexistentes; o, pueden haber sido desarrollados, pero carecen de parámetros de intercambio de información y generalmente o son individuales o no estructurados.

FORMATIVO

Ha tenido lugar un diálogo para determinar qué industrias y organismos son fundamentales para el ecosistema nacional cibernético; se ha establecido una comunidad informal de operadores de la ICN; es evidente un diálogo regular entre los niveles ejecutivos estratégicos y tácticos respecto de las prácticas de riesgo cibernético.

ESTABLECIDO

Se han definido las estrategias internas y externas formales de comunicación de la ICN y son coherentes en todos los sectores, con una estrategia de comunicación que ha sido avalada y con un punto de contacto claro; se han acordado la perspectiva de la política del gobierno, el proceso de toma de decisiones y la maquinaria para la gestión y garantía de la seguridad cibernética.

ESTRATÉGICO

Se ha establecido una campaña de sensibilización para facilitar la estrategia de comunicación de la ICN con un punto de contacto para obtener esta información; han sido claramente identificados y administrados los requisitos y vulnerabilidades de seguridad cibernética en los sistemas de abastecimiento de la ICN; se ha implementado un proceso de revisión de las vulnerabilidades.

DINÁMICO

Se ha creado confianza entre el gobierno y las ICN con respecto a la seguridad de datos e intercambio de información sobre amenazas, lo que sirve para la toma de decisiones estratégicas; la gestión de riesgos de seguridad cibernética es parte de la cultura organizacional y activamente refleja el entorno operativo de la red; miembros de la junta directiva de nivel C pueden tomar decisiones de gestión de riesgos con conocimiento de causa sobre la base de la inteligencia confiable comunicada con eficacia.

INICIAL

La conciencia acerca de amenazas por parte de los operadores de la ICN es mínima, o no existe en absoluto; las habilidades y comprensión básicas de gestión de riesgos pueden ser incorporadas en las prácticas empresariales, pero la seguridad cibernética está supeditada a las TI y el riesgo de protección de datos y no se reconoce más ampliamente.

FORMATIVO

Se ha avanzado algo en materia de capacitación y creación de conciencia a fin de que la gestión de incidentes se pueda aplicar de manera eficiente; se implementa el control de acceso y se proporciona formación; la industria de la ICN tiene capacidades básicas para detectar, identificar, proteger, responder y recuperarse de las amenazas cibernéticas, pero estas capacidades son descoordinadas y varían en calidad.

ESTABLECIDO

Se han establecido directrices sobre mejores prácticas cibernéticas de ICN y medidas de seguridad mínimas; se han definido procedimientos de respuesta a incidentes y todas las entidades apropiadas participan activamente; se registra la detección de amenazas internas; se ha establecido una base legal para la seguridad de la red de ICN (del lado del operador y del usuario); la aplicación de las normas de la ICN es monitoreada y revisada.

ESTRATÉGICO

La seguridad cibernética está firmemente arraigada en la práctica general de gestión de riesgos; se desarrollan medidas de seguridad para garantizar la continuidad del negocio de la ICN en el contexto del entorno de riesgo que prevalece; los recursos se asignan en proporción a la evaluación del impacto de un incidente para garantizar la puntualidad y la eficacia de la respuesta a incidentes.

DINÁMICO

Se implementan prácticas de auditoría periódicas para evaluar las dependencias de red y del sistema, lo que sirve de base para la reevaluación continua de la cartera de riesgo; se fomenta la autorregulación; están operando los procedimientos para optimizar el marco jurídico relativo a la ICN por medio de la modificación de la legislación existente o promulgación de nuevas regulaciones legales, según sea necesario.

Gestión de crisis

La gestión de crisis es más que la respuesta a incidentes. Ejercicios cibernéticos, por ejemplo, pueden simular una variedad de roles, desde atacantes a defensores, equipos de comunicación, organismos de coordinación y varios otros, todos los cuales son cruciales en caso de una crisis real. La planeación y la evaluación de las aplicaciones de gestión de crisis les ofrecen a los interesados la capacidad para hacerles frente a situaciones del mundo real.

Planeación

INICIAL

No hay entendimiento, o es mínimo, de que la gestión de crisis es necesaria para la seguridad nacional; se ha asignado en principio la autoridad de planeación y diseño del ejercicio, pero no se ha esbozado la planeación.

FORMATIVO

Se ha llevado a cabo una evaluación preliminar de las necesidades de las medidas que requieren comprobación, con la consideración de un escenario de ejercicio simple, con un tamaño, ámbito geográfico, recursos y coordinación limitados; están incluidos actores clave en el proceso de planeación.

ESTABLECIDO

Un escenario realista de alto nivel informa un plan para poner a prueba los flujos de información y toma de decisiones integral y nueva información alimenta el ejercicio en puntos clave; se utilizan monitores externos, o se les proporciona formación profesional a monitores internos.

ESTRATÉGICO

El proceso de planeación incluye objetivos específicos, medibles, alcanzables, realistas y de duración determinada (SMART, por sus siglas en inglés), Infraestructuras de Clave Pública (PKI, por sus siglas en inglés), la participación de los participantes, un esbozo de su papel en el ejercicio y la articulación de los beneficios y los incentivos para la participación; se desarrolla la confianza con bastante antelación a través del proceso de reclutamiento y el ejercicio previo, y mediante el control garantizado de la confidencialidad.

DINÁMICO

El programa de ejercicio es amplio en su alcance geográfico y participación, así como en complejidad política/técnica; el ejercicio aborda desafíos internacionales y produce resultados escalables para el desarrollo de políticas y toma de decisiones estratégicas; observadores externos participan y contribuyen al proceso.

Evaluación

INICIAL

No se ha realizado ninguna evaluación de los protocolos y procedimientos de gestión de crisis; los resultados de los ejercicios no informan a la gestión global de crisis.

FORMATIVO

Existe la conciencia general de las técnicas y metas de gestión de crisis; el ejercicio se evalúa y los participantes proporcionan comentarios sobre una base ad hoc, pero esto no alimenta la toma de decisiones.

ESTABLECIDO

Las partes interesadas están incluidas en el proceso de evaluación; se recogen indicadores medibles de éxito, incluyendo cuestionarios, pruebas repetidas, seguimientos y lecciones aprendidas; los resultados se cotejan, analizan y se introducen en el proceso de toma de decisiones; los resultados se evalúan sobre la base de las mejores prácticas de gestión de crisis a nivel nacional e internacional.

ESTRATÉGICO

SMART y PKI producen resultados estructurados, medibles, que redundarán en recomendaciones útiles para los responsables de las políticas y las partes interesadas; se preparan informes personalizados específicos al sector para cada grupo de interés, garantizando al mismo tiempo la seguridad de la información sensible; los resultados de la evaluación de gestión de crisis informan la implementación de estrategias nacionales y las asignaciones presupuestales.

DINÁMICO

Se le proporciona a la comunidad internacional la evaluación de la participación del país en los ejercicios internacionales de gestión de crisis, por lo que las lecciones aprendidas pueden contribuir a una comprensión global de la gestión de crisis.

Redundancia digital

En el escenario donde se desactiva la comunicación por medios electrónicos, es fundamental la creación de vínculos de coordinación de respaldo entre los servicios de emergencia que no se basan en redes digitales de comunicación para mejorar la política y la estrategia cibernética.

Planeación

INICIAL

Pueden considerarse o no medidas de redundancia digital.

FORMATIVO

Las partes interesadas se reúnen por medio de asociaciones público-privadas para identificar brechas y superposiciones en las comunicaciones de los activos de respuesta de emergencia y enlaces de autoridad; se establecen prioridades de activos de respuesta de emergencia y procedimientos operativos estándar en el caso de una interrupción de las comunicaciones a lo largo de cualquier nodo de la red de respuesta de emergencia.

ESTABLECIDO

Los activos de respuesta de emergencia están cableados en una red de comunicación segura; se asignan recursos adecuados para la integración de hardware, pruebas de estrés tecnológico y capacitación de personal y ejercicios de simulación de crisis.

ESTRATÉGICO

Se lleva a cabo divulgación y educación de los protocolos de comunicación redundantes para las principales partes interesadas y se las adapta a sus funciones y responsabilidades únicas.

DINÁMICO

Los interesados contribuyen a los esfuerzos internacionales sobre planeación de la comunicación de redundancia.

Organización

INICIAL

Los activos de respuesta de emergencia actuales no han sido identificados; si se identifican, carecen de cualquier nivel de integración.

FORMATIVO

Los activos de respuesta de emergencia se mapean y se identifican, posiblemente incluyendo detalles sobre su ubicación y sus operadores designados.

ESTABLECIDO

La comunicación se distribuye a través de las funciones de respuesta de emergencia, áreas geográficas de responsabilidad, respondedores públicos y privados y las autoridades de mando.

ESTRATÉGICO

Los activos de respuesta de emergencia prueban la interoperabilidad y funcionan con eficacia en escenarios y ejercicios de comunicación comprometidos; los resultados de estos escenarios luego sirven de base para la inversión estratégica en futuros activos de respuesta a emergencias.

DINÁMICO

Está operando la eficiencia optimizada para mediar cortes prolongados de sistemas; activos a nivel nacional pueden actuar para ayudar a los países vecinos en caso de una crisis o incidente a nivel internacional; se proponen, programan y llevan a cabo mapeos y simulacros de interoperabilidad de respuesta a emergencias sobre una base anual.

Mercado de la ciberseguridad

Este factor se refiere a la disponibilidad de tecnologías de seguridad cibernética de la información y red y apoyo especializado para el despliegue, y también al seguro cibernético como una forma de protección contra las pérdidas que afectan directamente al titular del seguro o contra las pérdidas de otra organización o individuos afectados por una falla de seguridad.

Tecnologías de seguridad cibernética

INICIAL

Poca o ninguna tecnología se produce en el país; pueden estar restringidas las ofertas internacionales o son vendidas con un sobreprecio.

FORMATIVO

La tecnología y los procesos de seguridad en el gobierno y el sector privado están disponibles y desplegados; el mercado interno ofrece productos genéricos, no especializados; las ofertas no están impulsadas por el mercado; consideraciones de seguridad están integradas en el software y la infraestructura.

ESTABLECIDO

Se crean y administran los sistemas de control de tecnología de la información; los productos de seguridad informática nacional provienen de proveedores locales; las tecnologías están desplegadas en el país para detectar y registrar incidentes cibernéticos, incluyendo ataques sofisticados; se implementan tecnología y procesos de seguridad avanzados en las redes empresariales sensibles para permitir el intercambio de información segura.

ESTRATÉGICO

Las tecnologías de seguridad cibernética, incluyendo el software, cumplen con las directrices de codificación segura, mejores prácticas y se acogen a las normas reconocidas internacionalmente; las tecnologías y procesos están actualizados a través de los sectores de seguridad, con base en la evaluación del riesgo estratégico; la evaluación de riesgos también sirve de base para la aplicación de los incentivos del mercado hacia productos priorizados a fin de mitigar los riesgos identificados.

DINÁMICO

Las características de seguridad en la arquitectura de software se actualizan continuamente a medida que se requiere; las funciones de seguridad en las configuraciones de sistemas informáticos y software están automatizadas en el desarrollo y despliegue de soluciones de seguridad; la dependencia nacional de tecnologías extranjeras se mitiga a través de la capacidad nacional mejorada; el mercado nacional de productos de seguridad cibernética se exporta a otros países y se consideran productos de calidad superior.

Seguros de delincuencia cibernética

INICIAL

La necesidad de un mercado para los seguros de delincuencia cibernética no ha sido identificada a través de la evaluación de riesgos financieros para el sector público y privado.

FORMATIVO

Se ha identificado la necesidad de un mercado para los seguros de delitos informáticos a través de la evaluación de riesgos financieros para los sectores público y privado; ahora se está discutiendo el intercambio de las mejores prácticas en materia de evaluación y reducción de riesgos, incluyendo el desarrollo y uso de estándares y productos variados apropiados.

ESTABLECIDO

Se ha establecido el mercado para los seguros de la delincuencia cibernética y se fomenta el intercambio de información entre los participantes; se ofrecen productos adecuados para las PYME.

ESTRATÉGICO

El seguro cibernético especifica una variedad de coberturas para mitigar pérdidas consecuentes; estas coberturas son seleccionadas en base a las necesidades de planeación estratégica y de riesgo identificadas.

DINÁMICO

Existe un mercado vibrante, innovador y estable de seguros de cibernética y se adapta a los riesgos emergentes; constantemente se revisan y mantienen los programas de reducción de riesgo planeados; se ofrecen primas de seguros y programas de recompensas para el comportamiento cibernético seguro constante; los productos de seguros están alineados con las aplicaciones dinámicas de las normas y prácticas de seguridad cibernética.